

(51) International Patent Classification <sup>6</sup> : G06F 153/00		A1	(11) International Publication Number: WO 99/46720
			(43) International Publication Date: 16 September 1999 (16.09.99)
(21) International Application Number: PCT/US99/05368		(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).	
(22) International Filing Date: 11 March 1999 (11.03.99)			
(30) Priority Data:			
60/077,635 11 March 1998 (11.03.98) US			
09/260,874 2 March 1999 (02.03.99) US			
(71) Applicant: CHA! TECHNOLOGIES SERVICES, INC. [US/US]; 2nd floor, 704 Broadway, New York, NY 10003 (US).			
(72) Inventors: LEITERSDORF, Yoav, A.; 2nd floor, 704 Broadway, New York, NY 10003 (US). SIXTUS, Timothy; 2nd floor, 704 Broadway, New York, NY 10003 (US).		Published <i>With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i>	
(74) Agents: KALOW, David, A. et al.; Kalow Springut & Bressler, 19th floor, 488 Madison Avenue, New York, NY 10022 (US).			

# BEST AVAILABLE COPY

324

322

EXTRA SERVERS TO SCALE

310

312

314

316

318

320

322

Q

BANKER/MEMBERSHIP

RRDB

chaSM

chaNGE WEB

CONTENT WEB

ACCOUNT WEB

CREDIT CARD PROCESSOR

332

REPLENISHMENT

334

SWITCH

340

330

328

ACCOUNTING SYSTEM

DATA MINING SYSTEM

326

324

chaNGE / TRANSACTION LOG DATABASE

ACCOUNT DATABASE

306

INTERNET

304

BUYER

BUYER

BUYER

BUYER

302

MERCHANT

MERCHANT

300

— INTERNAL NETWORK CONNECTION  
 - - - EXTERNAL NETWORK CONNECTION  
 . . . TRANSACTION QUEUE CONNECTION

**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakhstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

## AUTOMATICALLY INVOKED INTERMEDIATION PROCESS FOR NETWORK PURCHASES

### FIELD OF THE INVENTION

5 This invention relates to online electronic communications and transactions, and, in particular, to transactions between resource providers and users of such resources that communicate in an internetworked computer system.

### BACKGROUND ART

10 Internetworked computer systems, such as the Internet, allow transactions such as electronic commerce purchases including electronic resource acquisition. In fact, the Internet has quickly become the preferred choice of many users for obtaining information, data, images, sound clips, software programs, etc. (referred to generally as a resource) since a user has virtually unlimited access to any host computer connected to the Internet. Problems have arisen, however, that are somewhat unique to this electronic commerce paradigm.

15 For instance, one problem has arisen in the area of authentication or confirmation of a user's identity. That is, when a user wishes to access a resource provided by a resource provider, the resource provider must be able to ensure that the user is actually who she says she is. In the real world, the provider (e.g., a shopkeeper) can simply ask for a driver's license or other piece of identification to confirm the shopper's identity prior to accepting payment in the form of a check or credit card. In the online environment, other forms of identification are  
20 obviously required.

One unique method of accomplishing such authentication in the online environment is described in detail in co-pending United States patent application serial no. 08/816,410,

assigned to the assignee of the present invention, which is incorporated by reference herein. In that application, a unique triangulation methodology is presented, in which a trust server is utilized to confirm to a requesting online party the identity of another online party that was previously registered with the trust server. This is of course useful in the e-commerce application, wherein the purchaser can pre-register with the trust server and subsequently request an online vendor to execute a purchase transaction. The online vendor requests authentication of the purchaser from the trust server, and a three-way data exchange and confirmation process takes place. After confirmation, the online purchase transaction can be consummated.

Another problem that exists in the online world is the instance wherein a user would like to obtain a resource from a resource provider, such by downloading an image or other piece of information. Many resource providers require users to be registered with their services, for example by paying a monthly fee of \$20.00 for unlimited downloading of data. The user may not want have to pay for such subscriptions just to get a single resource, especially since the cost of such registrations can become quite expensive given the number of resource providers that exist on the Internet.

In spite of a number of drawbacks, the Internet digital communications network is widely used for commercial transactions in which a buyer accesses a web site of a merchant using a browser and purchases data, textual material, graphics, or other digital content for immediate delivery from the merchant's site to the purchaser's site over the network. Often the content purchased is relatively inexpensive, say under a dollar in price. Nonetheless, heretofore large programs at both the buyer's site and the merchant's site have been required to handle the financial aspects of the transaction. Payments for purchases made over the network have been conventionally made with a digital currency known as "e-cash" using a

program at the buyer's site known as "wallet" software that is cumbersome to use and makes heavy use of encryption technology, which tends to lengthen the time required to complete the transaction. Transfer of any amount of e-cash, however small, from a buyer to a merchant has had to be cleared by a third-party bank or other financial institution. From the purchaser's perspective, the requirement to use wallet software and e-cash to purchase content over the network makes such purchases a "hassle," particularly in the case of inexpensive purchases, which has tended to discourage potential purchasers from making such purchases. On the merchant's side, difficulties often have been encountered in coordinating the clearance of the buyer's e-cash payment by the merchant's payment processing software and the transmission of the content purchased to the purchaser by web publication software at the merchant's site.

United States patent No. 5,767,917 to Rose *et al.* ("the Rose *et al.* '917 patent") disclosed a computerized payment system for purchasing goods and services on a quasi-public network such as the Internet. As disclosed at column 3, line 51 through column 4, line 14 of the '917 patent, the payment system included an "above-the-line system" and a "below-the-line system" which were separated by a "firewall" which isolated the two systems from one another. The above-the-line system included computer hardware and software directly connected to the Internet and represented the non-secure side of the firewall. The below-the-line system included computer hardware and software and was connected to the above-the-line system via a private network. The private network permitted limited communication between the two systems, but prevented unauthorized access to the below-the-line system through the above-the-line system. The below-the-line system represented the secure side of the firewall.

According to column 4, lines 46 through 52 of the Rose *et al.* patent, the above-the-line system ran an above-the-line program which provided communication with users on the Internet who were buyers and users on the Internet who were sellers. As disclosed at column 4, line 66 through column 5, line 9 of the '917 patent, a buyer could access the above-the-line program interactively over the Internet by using a user-interface software program that could

be run on the user's computer, or could access the payment system via a conventional e-mail program. A seller could access the above-the-line program over the Internet interactively by running an interface software program on the seller's computer or could access the payment system via a conventional e-mail program.

5 As disclosed at column 5, lines 17 through 25 of the Rose *et al.* '917 patent, in order for an Internet user to use the payment system of the patent as either a buyer or a seller, the user would have to establish an account with the payment system. According to column 5, lines 35 through 64 of the patent, a buyer's account - termed a "cardholder" account - would include (1) a cardnumber which would identify the account, (2) the cardholder's name, (3) the  
10 cardholder's Internet e-mail address, (4) the state of the account; *i.e.*, "active," "suspended," or "invalid;" and (5) a pay-in selection indicating how the cardholder would make payment; *e.g.*, authorization to charge a credit card. It was stated at column 5, lines 63 and 64 of the '917 patent that the pay-in selection was neither encoded in nor directly derivable from the cardnumber of the account. At column 6, line 51 through column 7, line 12 of the patent, it  
15 was disclosed that only a portion of the buyer cardholder account information resided in the above-the-line system of the payment system of the patent. Specifically, the account number, the cardholder's name, the Internet e-mail address of the cardholder, and the state of the account were stored in the above the line computer. The above-the-line computer did not contain pay-in information such as credit card information. A full copy of all the buyers'  
20 cardholder account information resided in the below-the-line system.

According to column 6, lines 41 through 50 of the Rose *et al.* '917 patent, a seller's account with the payment system of the patent would include the following data: (1) a seller's account cardnumber, (2) the seller's name, (3) the seller's Internet e-mail address, (4) a state of the account, and (5) a seller's agent number. As disclosed at column 6, lines 15 through 37  
25 of the patent, a seller's agent would be a bank card processor which would interact with credit card bureaus to perform the functions of credit card authorizations and chargebacks. The seller's agent number would be stored in the below-the-line system of the payment system of the patent, and not in the above-the-line system. See column 7, lines 17 through 20 of the Rose *et al.* '917 patent.

As disclosed at column 8, lines 1 through 26 of the Rose *et al.* '917 patent, when a buyer decided to buy goods or services from a seller, the buyer would inform the seller of the buyer's cardnumber by means of an appropriate message over the Internet. Upon receiving the buyer's message, the seller would send a payment-request message to the payment system of the patent over the Internet, either by e-mail or by an interactive protocol on the Internet. The payment-request message from the seller would include the buyer's cardnumber, the seller's cardnumber, a textual description of the transaction, an amount, a merchant's transaction identifier, and any delivery information. According to column 6, lines 27 through 38 of the '917 patent, after receiving the payment-request message, the above-the-line program would ascertain whether the message was from a qualified seller by checking a database file on the above-the-line system. Upon confirmation that the payment-request message was from a qualified seller, the above-the-line program of the payment system of the patent would generate a payment-query message to be sent to the buyer over the Internet to ask the buyer whether the buyer authorized payment for the transaction to the seller.

According to column 8, lines 40 through 62 of the Rose *et al.* '917 patent, the payment-query message contained a transaction identifier, the buyer's name, the seller's name, the textual description of the transaction, and an amount. The payment-query message would then be sent to the buyer's e-mail address.

As disclosed at column 8, lines 62 through 64 of the Rose *et al.* '917 patent, the payment-query message would request the buyer to respond with one of three replies: "yes," "no," or "fraud." According to column 10, lines 31 through 66 of the patent, if the buyer responded with a message indicating "yes," the above-the-line program would transfer the transaction information to the below-the-line program. When the transaction information was received, the below-the-line system would associate the buyer's cardnumber with the buyer's payment information and the seller's account number with the seller's agent number. The below-the-line system would then communicate to the seller's agent the identity of the seller, the transaction amount, the buyer's credit card number or other payment information, and any delivery information. The communication to the seller's agent would be carried out on secure communication channels off the Internet. If the seller's agent approved the charge, it would send an authorization code to the below-the-line system. According to column 10, lines 64

through 66 and column 11, lines 8 through 25 of the Rose *et al.* '917 patent, upon receipt of the authorization code, the below-the-line program would generate a cryptographic signature for the authorization code which would then be transferred to the above-the-line program.

5 The above-the-line program would then transmit to the seller a payment-notification message which would include the seller's transaction identifier and the cryptographically signed authorization code. Upon receipt of the payment-notification message, the seller could cryptographically authenticate the authorization code and, upon verification of the authenticity of the message, proceed to deliver the goods or services to the buyer. According to column 11, lines 26 through 32 of the Rose *et al.* '917 patent, further processing of the charges to the  
10 buyer's credit card account and credits to the seller's merchant account would be conducted by a conventional settlement system off the Internet, reportedly isolating the buyer-seller activity which occurred on the Internet from the financial and credit activity which occurred off the Internet.

United States patent No. 5,822, 737 to Ogram ("the Ogram '737 patent") concerned  
15 an automated payment system for purchases over a distributed computer network such as the Internet. According to column 4, line 57 through column 5, line 4 of the '737 patent, a consumer using a customer computer would connect with a merchant computer over the network. The merchant computer would communicate promotional material to the customer computer via the network. If the customer decided to buy the service or product from the  
20 merchant, the link with the merchant computer would be broken - by a mechanism apparently not specified in the '737 patent - and the customer computer would be linked with a payment processing computer. In the change from the merchant computer to the payment processing computer, an indicia of the URL or the product being promoted by the merchant computer would be communicated to the payment processing computer. The payment processing  
25 computer could accept the credit card account number which was to be debited the amount of the product. Column 5, lines 22 through 24 of the '737 patent. According to column 2, lines 7 through 10 of the patent, an encrypting software package could be first downloaded to the customer's computer for secure transmission of the credit card number. As disclosed at column 5, lines 25 through 33 of the Ogram '737 patent, the payment processing computer  
30 would then establish a link via telephone lines with a credit card server computer while



maintaining linkage with the customer computer. The credit card account number and amount would be communicated to the credit card server computer, which would respond with an authorization indicia.

According to column 2, lines 16 through 37 of the Ogram '737 patent, after receipt of the authorization indicia, the payment processing computer would in certain cases transmit a password to the customer's computer. The password would have been defined by the merchant's computer to pass along to the customer's computer. The password could be used by the customer's computer to gain access to restricted material within the merchant's computer. As disclosed at column 6, lines 25 through 34 of the Ogram '737 patent, the password could be displayed on a window in a screen on the customer's computer for the customer to use with the merchant. The password could be printed or committed to memory, and then entered by the consumer to lift restricted access to material in the merchant's computer.

## SUMMARY OF THE INVENTION

The subject invention broadly concerns an automatically invoked intermediation process for purchasing content over a digital communications network by subscribing purchasers from subscribing merchants.

The intermediation process comprises the step of establishing a database of subscriber-purchaser accounts and a database of subscriber-merchant accounts at a central transaction processing site on the digital communications network. The subscriber-merchant accounts database includes information encoding resource locator data identifying at least one restricted-access port at each subscribing merchant site on the network and, for each such restricted-access port, information encoding an access fee schedule for accessing content by way of the restricted-access port and access-restriction-override information such as a password for enabling access to content by way of the restricted-access port. The subscriber-purchaser accounts database includes information encoding purchaser site authentication credentials and a purchaser account balance for each subscribing purchaser.

The intermediation process of the invention further comprises establishing a resource rules database at the network site of each subscribing purchaser. The resource rules database includes information encoding resource-locator-data identification criteria corresponding to each of at least a subset of the restricted-access ports at subscribing merchant sites identified in the subscriber-merchant accounts database and the access fee schedule for accessing content by way of the corresponding restricted-access port.

The intermediation process of the invention also includes the steps of locally monitoring network communication activity information at the network site of each subscribing purchaser with respect to access to a target network resource generated by a browser program at the subscribing purchaser site and comparing such network communication activity information to the resource-locator-data identification criteria corresponding to restricted-access ports at the network sites of subscribing merchants in the resource rules database locally maintained at the site of the subscribing purchaser.

In the event network communication activity information pertaining to the target network resource matches with the resource-locator-data identification criteria corresponding to a restricted-access port in the resource rules database, the intermediation process of the invention also includes the steps of retrieving the access fee schedule corresponding to the matched resource-locator-data identification criteria from the resource rules database, displaying an access fee from the access fee schedule for accessing content by way of the restricted access port corresponding to the resource-locator-data identification criteria, and prompting for approval or disapproval of completing the access for the displayed access fee.

The intermediation process of the invention further comprises, upon receipt at the subscribing purchaser site of a user communication responsive to the prompting indicating approval of completing the access to content by way of the restricted-access port for the access fee, the step of transmitting a purchase-request message from the subscribing purchaser site to the transaction processing site over the network. The purchase-request message includes information encoding purchaser-site authentication credentials and identifying the

restricted-access port at the merchant site corresponding to the matched resource-locator-data identification criteria.

The intermediation process of the invention also comprises, upon receipt of the purchase-request message at the transaction processing site, the step of determining whether the purchaser-site authentication credentials encoded in the purchase-request message matches with any purchaser-site authentication credentials included in the subscriber-purchaser accounts database. If such a match is found, the process of the invention includes the step of transmitting over the network to the restricted-access port of the merchant site a restricted-access-enabling access-request message to download purchased content by way of the restricted-access port to the transaction processing site. The restricted-access-enabling access-request message includes access-restriction-override information corresponding to the restricted-access port retrieved from the subscriber-merchant accounts database.

The intermediation process of the invention further comprises, upon receipt of the downloaded purchased content at the transaction processing site from the subscribing-merchant site by way of the restricted-access port responsive to the restricted-access-enabling access-request message, the steps of encrypting the downloaded purchased content and forwarding the thus encrypted purchased content to the subscribing purchaser site over the network.

The intermediation process of the invention also includes, upon receipt of the encrypted purchased content at the subscribing purchaser site, the step of transmitting a content-received confirmation message to the transaction-processing site by the subscribing purchaser site over the network.

The intermediation process of the invention further includes, upon receipt of the content-received confirmation message from the subscribing purchaser site at the transaction processing site, the step of debiting the purchaser account balance corresponding to the subscribing purchaser in the subscriber-purchaser accounts database by the access fee for accessing purchased content by way of the restricted-access port and forwarding a

cryptographic key for decrypting the encrypted purchased content to the subscribing purchaser site over the network.

Finally, the intermediation process of the invention includes, upon receipt of the cryptographic key at the subscribing purchaser site, the step of decrypting the encrypted purchased content at the purchaser site.

Preferably, the access fee schedule corresponding to a restricted-access port in the subscriber-merchant accounts database consists of a single access fee for accessing content by way of the restricted-access port.

The access-restriction-override information corresponding to a restricted-access port in the subscriber-merchant accounts database preferably includes a password for enabling access to content by way of the restricted-access port.

The subscriber-purchaser accounts database preferably includes, for each subscribing purchaser, information encoding an account-replenishment amount and a financial account number identifying an account at a financial institution upon which the subscribing purchaser may draw. The step of debiting the purchaser account balance corresponding to the subscribing purchaser in the subscriber-purchaser accounts database by the access fee for accessing purchased content by way of the restricted-access port preferably includes the step of comparing the purchaser account balance with an account minimum value. If the purchaser account balance has fallen below the account minimum value, the process of the invention preferably includes the step of sending a funds-transfer request to the financial institution for transferring funds in the amount of the account-replenishment amount from the account identified by the financial account number to an intermediation entity account. Upon receipt at the transaction processing site of an approval of the transfer request, the purchaser account balance is preferably credited by the account replenishment amount to bring the purchaser account balance above the account minimum value.

The funds transfer request is preferably sent from the transaction processing site to the financial institution over a communication channel separate from the digital communications network interconnecting the transaction processing site, the subscribing purchaser sites, and the subscribing merchant sites.

5           The digital communications network interconnecting the transaction processing site, the subscribing purchaser sites, and the subscribing merchant sites is preferably the Internet.

Content purchased by means of a preferred intermediation process of the invention can include practically any resource which can be transmitted over the Internet. Such content could include text, software, data, visual images, and audio, for example.

10           Certain types of digital content such as hypertext mark-up language ("HTML") documents frequently contain embedded software objects such as images encoded in a standard format such as the graphic image format ("GIF") or the joint photographic experts group ("JPEG") format. A software object embedded in digital content is conventionally identified by resource locator data such as a URL which encodes the location of the object on  
15 the network. In a preferred embodiment of the intermediation process of the invention, digital content downloaded to the transaction processing site from a restricted-access port of a subscribing-merchant site is checked to determine if the content is of a type likely to contain embedded software objects. If the content is found to be an HTML document or other type of content likely to contain embedded software objects, the content is parsed at the transaction  
20 processing site and any resource locator data corresponding to a software object embedded in the content extracted. Resource locator data so extracted is then used to retrieve any corresponding software objects over the network. The software objects thus retrieved are combined with the original downloaded content at the transaction processing site to form a composite purchased-content object. The composite purchased-content object is then  
25 encrypted and forwarded to the subscribing purchaser site which purchased the content over the network. Decryption of the encrypted composite purchased-content object at the subscribing purchaser site according to such preferred process makes available the original content and any embedded software objects at the purchaser site without the necessity of the

browser running on the purchaser site having to retrieve the embedded software objects over the network.

Optionally, if suitable arrangements are made with the subscribing merchant, a copy of a digital content downloaded to the transaction processing site from a restricted-access port at the network site of the subscribing merchant pursuant to a purchase-request message received from a subscribing purchaser site in accordance with an embodiment of the intermediation process of the invention may be cached at the transaction processing site. If a purchaser-request message is received subsequently from a second subscribing purchaser site which identifies the same digital content as that cached in the transaction processing site, the cached copy of the digital content may be used to provide the purchased content for encryption and downloading to the second subscribing purchaser site without having to access the content a second time by way of the restricted-access port of the subscribing merchant port.

In addition to digital content transmitted over the Internet, "hard goods" may be purchased by subscribing purchasers from subscribing merchants over the Internet for delivery offline by means of a preferred intermediation process of the invention described in the following paragraphs.

The preferred automatically invoked intermediation process for purchasing hard goods over a digital communications network such as the Internet includes the steps of establishing a database of subscriber-purchaser accounts and a database of subscriber-merchant accounts at a central transaction processing site on the network. The subscriber-merchant accounts database includes information encoding resource locator data identifying at least one order-entry port at each subscribing merchant site on the network and, for each such order-entry port, information encoding a schedule of prices and goods purchasable by orders entered by way of the order-entry port. The subscriber-purchaser accounts database includes information for each subscribing purchaser encoding purchaser site authentication credentials and a purchaser account balance.

The intermediation process for purchasing hard goods also includes the step of establishing a resource rules database locally at the network site of each subscribing purchaser. The resource rules database includes information encoding resource-locator-data identification criteria corresponding to each of at least a subset of the order-entry ports at subscribing merchant sites identified in the subscriber-merchant accounts database and the schedule of prices and goods purchasable by orders entered by way of the corresponding order-entry port.

The intermediation process for purchasing hard goods further includes the steps of locally monitoring network communication activity information at the network site of each subscribing purchaser with respect to access to a target network resource generated by a browser program at the subscribing purchaser site and comparing such network communication activity information to the resource-locator-data identification criteria corresponding to order-entry ports at the network sites of subscribing merchants in the resource rules database locally maintained at the site of the subscribing purchaser.

In the event network communication activity information pertaining to the target network resource matches with the resource-locator-data identification criteria corresponding to an order-entry port in the resource rules database, the intermediation process for purchasing hard goods also includes the steps of retrieving the schedule of prices and goods corresponding to the matched resource-locator-data identification criteria from the resource rules database, displaying at least a portion of prices and goods from the schedule, and prompting for identification of goods to be ordered.

The intermediation process of the invention for purchasing hard goods further comprises, upon receipt at the subscribing purchaser site of a user communication responsive to the prompting identifying hard goods to be ordered, the step of transmitting an order-request message from the subscribing purchaser site to the transaction processing site over the network. The order-request message includes information encoding purchaser-site authentication credentials, identifying the order-entry port at the merchant site corresponding to the matched resource-locator-data identification criteria, and specifying the hard goods to be ordered.

The intermediation process of the invention for purchasing hard goods also comprises, upon receipt of the order-request message at the transaction processing site, the step of determining whether the purchaser-site authentication credentials encoded in the order-request message matches with any purchaser-site authentication credentials included in the subscriber-purchaser accounts database. If such a match is found, the process includes the step of transmitting over the network to the order-entry port of the merchant site an order-entry message to enter an order for the hard goods specified in the order-request message by way of the order-entry port and request transmission of an order-confirmation message from the merchant site to the transaction processing site.

10 The intermediation process of the invention for purchasing hard goods further includes, upon receipt of an order-confirmation message at the transaction processing site from the subscribing merchant site responsive to the order-entry message, the steps of encrypting the order-confirmation message and forwarding the encrypted order confirmation message to the subscribing purchaser site over the digital communications network.

15 The intermediation process of the invention for purchasing hard goods also includes, upon receipt of the encrypted order-confirmation message at the subscribing purchaser site, the steps of transmitting an order-confirmation received message to the transaction-processing site by the subscribing purchaser site over the network.

20 The intermediation process of the invention for purchasing hard goods further includes, upon receipt of the order-confirmation message from the subscribing purchaser site at the transaction processing site, the step of debiting the purchaser account balance corresponding to the subscribing purchaser in the subscriber-purchaser accounts database by the total price of the hard goods ordered and forwarding a cryptographic key for decrypting the encrypted order-confirmation message to the subscribing purchaser site over the network.



The intermediation process of the invention for purchasing hard goods also includes, upon receipt of the cryptographic key at the subscribing purchaser site, the step of decrypting the encrypted order-confirmation message at the purchaser site. Delivery of the hard goods to the subscribing purchaser is made offline by the subscribing merchant. The decrypted order-confirmation message may be used as proof to the subscribing merchant that the goods were ordered and paid for.

Advantageously, a subscribing merchant to an intermediation service carrying out a preferred intermediation process of the invention can use conventional Web publishing software at its Internet site to establish publicly accessible ports and restricted-access ports for use in connection with the intermediation process. Commercially available conventional Web publishing software ordinarily has facilities for establishing a password-protected restricted-access port at an Internet site which requires the presentation of a user identification code and a password to obtain access to content by way of the restricted access port. No software in addition to such conventional Web publishing software is required of a subscribing merchant to make use of preferred intermediation processes of the invention, which represents a significant advantage over the prior art.

In one aspect of the present invention, the problem of the user needing subscriptions in order to obtain online resources is addressed through the use of a resource proxy.

The resource proxy acts as a broker, and generally will have its own subscriptions to many resource providers. When a user requests a resource from a provider, a client process on the user's machine intercedes and requests the resource proxy to obtain the resource. In one preferred embodiment of the invention, the client process intercedes when the provider asks for the user's identification and password in response to a request for a resource by the user. In an alternative preferred embodiment of the invention, the client process intercedes when the user generates a request to access a resource from a provider to which access is restricted. The resource proxy, who has an account with the resource provider (or who will get the account if required), then obtains the resource on behalf of the user and provides the resource to the user. Thus, the user can obtain many individual resources from the proxy

without having to subscribe to each service. The resource proxy can serve multiple users, of course, in order that the provision of such individual resources can make economic sense.

5 In another aspect of the present invention, a secure micropayment system is implemented by the resource proxy and the users to effect payment for the use of the resources.

10 In another aspect of the present invention, some aspects of the above-described triangulation methodology are used to implement unique and novel applications in the online environment. That is, the resource proxy may use a trust server to ensure that the requesting user is actually who she says she is, and to collect payment (the micropayment system) for the provision of the individual resource.

#### **BRIEF DESCRIPTION OF THE DRAWINGS**

Preferred embodiments of the intermediation process for network purchasers of the invention will be described below with reference to the following figures:

15 Figure 1 is an illustration of a triangulation authentication methodology utilized in a first preferred embodiment of the present invention.

Figure 2 is an illustration of a prior-art resource request made by a user to a resource provider.

Figure 3 is an illustration of the use of a resource proxy in the triangulation authentication schema of Figure 1.

20 Figures 4-7 and 9 illustrate the interaction between existing financial networks, resource providers, and the triangulation authentication flow.

Figure 8 illustrates resource acquisition in accordance with a preferred embodiment of the present invention.

Figure 10 is an illustration of one aspect of the use of a resource proxy in accordance with a preferred embodiment of the present invention.

Figure 11 illustrates data flow in a back office transaction.

Figures 12A-12C is a sample merchant application.

5        Figure 13 shows aggregation of micropayment sums.

Figure 14 is a schematic diagram of subscribing purchaser sites, subscribing merchant sites, and an intermediation service transaction processing site interconnected via the Internet for carrying out a preferred embodiment of the intermediation process of the invention.

10       Figure 15 is an illustration of an intermediation-service subscription application screen generated by a preferred intermediation service.

Figure 16 is an illustration of a subscription-confirmation screen generated by the preferred intermediation service.

Figure 17 illustrates a newspaper contents screen for a hypothetical online financial newspaper.

15       Figure 18 illustrates a newspaper subscription screen presented by the online financial newspaper when a Web browser attempts to navigate to restricted-access content of the newspaper without making use of a preferred intermediation service of the invention.

20       Figure 19 illustrates an intermediation-service pop-up window which appears on the screen of a subscribing purchaser's personal computer when a browser running on the computer attempts to access restricted-access content of the online financial newspaper in the case in which the newspaper is a subscribing merchant to the preferred intermediation service.

Figure 20 is an illustration of a screen representing content of the online financial newspaper to which access is restricted.

Figure 21 is an illustration of an account-maintenance screen presented to subscribing purchasers to the preferred intermediation service.

5     **DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS**

The following name table will facilitate understanding of micropayment system for one preferred intermediation process of the invention as presented herein.

Alice: Registered user running micropayment system client software.

Bob: Registered Server and Resource Proxy.

10     Ted: Trust Server / Broker.

Reg: Registration Server.

Hal: Resource Vendor, not necessarily associated with the system.

$S_A$ : A unique "secret" Alice shares with Ted.

$S_B$ : A unique "secret" Bob shares with Ted.

15      $R_A$ : Random number generated by Alice.

$R_B$ : Random number generated by Bob.

NGE Nonce Generation Event in which a session key (or nonce) is created to encrypt/decrypt requested resources.

K Random session key.

$K_A, K_B$  Function of one seed A to seed B, and it's inverse.

$F_{A1}-F_{AN}$  Results 1 through N of a function calculated by A.

$F_{B1}-F_{BN}$  Results 1 through N of a function calculated by B.

5 Referring to Figure 1, a triangulation authentication data flow over a computer network such as the Internet that will accomplish a successful authentication via a process referred to as a session manager is as follows:

1. User network site Alice initializes and sends an authentication request to user network site Bob.
- 10 2. User Bob accepts the authentication request, forms a first compound message comprising the authentication request and information about himself, and forwards the compound message to network site Ted.
3. Ted receives the first compound message (from Alice to Ted through Bob), confirms Alice's intent and sends her a second compound message to Bob
- 15 (from Ted to Bob through Alice).
4. Alice forwards Ted's message to Bob.

20 Encryption may optionally be utilized at sensitive message transfers to ensure that no data is viewed or tampered with by any party other than the intended recipient. This includes the compound messages Bob or Alice conveys. At step four, for example, the message Alice sends to Bob from Ted is preferably Ted's confirmation of Alice's status encrypted such that only Bob can decipher the message.

Based on this process, Bob can be a server with resources that Alice seeks or requires. Once the authentication is complete, Bob can serve Alice's requests with impunity.

Under standard HTTP protocol, a resource or resources that are made available via Web subscription are in most cases protected with a simple User ID/Password ("UID/PW") scheme. HTTP defines this type of protection in a straightforward manner. Referring now to Figure 2:

- 5           1.     Alice requests a World Wide Web resource by entering a Uniform Resource Locator ("URL") into her browser.
2.     The HTTP server ("Hal") fetches the resource for her request and returns it to her browser. However, if the resource is protected, Hal sends back a request for a UID/PW.
- 10       3.     In the latter case, the browser responds to Hal's request by displaying a dialog box with input boxes for a UID/PW pair.
4.     Alice's browser makes a second request for the resource, this time providing the user-entered UID/PW data with the request.
5.     Hal then fetches the resource for Alice's request and returns it to her browser.
- 15       After the initial UID/PW exchange, the entered data is stored during the rest her session to satisfy any of Hal's future requests for them.

Utilizing the triangulation authentication that the session manager facilitates, and the prior-art authentication model of HTTP's UID/PW scheme detailed above, a method for conducting micro-currency transactions is detailed, referred to herein as the micropayment system. Simply stated, in a triangulated system where Bob is a subscriber to an online service or has a previous relationship with a resource vendor, any Alice can obtain password-protected data through Bob's subscription or account without a subscription of her own.

Thus, in the process shown in Figure 3 (again, all data communication is over the Internet):

- 25       1.     Alice requests "any resource" from Hal.
2.     The resource is password protected, so Hal asks Alice for a password (PW).

3. The password request triggers the micropayment system control (the micropayment system control "captures" the password request and initializes the authentication process. Simultaneously, the URL is requested of Bob instead of Hal).

- 5        4. Alice asks Bob for "any resource", and sends triangulation authentication data.
5. Bob asks Ted if Alice is who she claims to be.
6. Ted checks, and sends Alice a compound message.
7. Alice forwards Bob's part of the message to Bob.
8. Bob is satisfied that Alice is really Alice, so he uses his account to request "any
- 10        resource" from Hal (Bob provides his own UID/PW data).
9. Hal delivers the resource to Bob.
10. Bob sends the resource on to Alice.

Finally, since Bob is a trusted member of Ted's network through prior registration, there exists a running dialog between the two. Ted can keep track of Alice's requests and

15        debit her account per delivery.

In Figure 4, all major components are shown and the overall data flow is outlined.

The platform of the present invention provides low cost, easy to use e-Commerce controls. The components are based on the foundation of Session Manager authentication, a process by which any registered user can authenticate himself or herself to any other in the

20        system.

The micropayment system facilitates online purchases of primarily digital resources that may range in value from less than a tenth of a cent to approximately US\$15.00. The upper bound may be determined by the abilities of Secure Electronic Transactions ("SET") initiatives.

25        Referring to Figure 4, prior to accessing any of the services that the system offers, Alice must register with Ted in the following manner:

1. Alice obtains the micropayment system client software via web link, download, CDROM, special offer or some other such means.
2. Alice runs an install program, and she is prompted to fill in her registration information.
- 5 3. The client software sends a Registration server (Reg) the appropriate information along with an approved fiscal instrument to charge (*e.g.*, a credit card account number).
4. Reg passes the registration data across a secure gateway to back-office services and generates a unique registration number for Alice.
- 10 5. Alice's fiscal instrument is charged a previously negotiated amount.
6. Upon a successful transaction, Alice's funds are credited to an account in the Bank and an "ok" status is returned to Reg from across the secure gateway.
- 15 7. The negotiated amount is digitally translated into NGE (Nonce Generation Events, that allow for decryption of resources to be provided in the future, and once used, represent a purchase) which are stored on a Trust Server (Ted) and associated with Alice's registration number.
8. Reg provides Alice with the registration number via a secure channel.
- 20 9. Alice activates her micropayment system client software and becomes a registered user.

Reg is not heard from again by this particular Alice, except in rare, well-defined cases discussed below.

Now Alice, as a registered user of the system, is micropayment system enabled and can make micro-currency purchases on the Internet. When Alice comes across a resource that she  
25 wants while browsing the Web, she simply has to click on it, or otherwise attempt to retrieve it as is her custom. If the resource vender (Hal) chooses to charge for accessing this resource, he will devise a mechanism to obtain proper credentials from anyone wanting the resource, as known in the art. In one preferred embodiment of the invention, Hal's request for credentials signals the micropayment system client to intercede on Alice's behalf. Alice is asked if she



would like Micropayment System to handle the transaction for her. If she agrees, then the resource request (URL) and authentication information is passed to a registered resource proxy. There exist user-configurable parameters such that Alice does not get bombarded with session manager conversation.

5           The session manager process is then initialized. Figure 5 shows the session manager authentication triangle (Alice to Bob to Ted to Alice, back to Bob).

The data flow to accomplish a successful authentication via a preferred session manager process is as follows:

1. Alice initializes and sends an authentication request to Bob.
- 10   2. Bob accepts this request, forms a first compound message comprising Alice's authentication request and information about himself, and forwards that first compound message to the trust server (Ted).
3. Ted receives the first compound message (from Alice to Ted through Bob), confirms Alice's intent and sends a second compound message
- 15   15   (from Ted to Bob through Alice).
4. Alice forwards Ted's message to Bob.

Encryption may be utilized at sensitive message transfers to ensure that no data is viewed or tampered with by any party other than the intended recipient. In particular, the compound message Ted sends in step three is preferably encrypted. A compound message

20   involves all three participants, and during each compound message transfer, the party in the middle adds or reads information unique to itself.

At step four, the message Alice sends to Bob from Ted is Ted's encrypted confirmation of Alice's status that only Bob can decipher. When Bob opens his message from Ted, he can be certain that Alice is who she claims to be.

Extending on this process, Bob can be a server with resources that Alice seeks or requires. Once the authentication is complete, Bob can serve Alice's requests with impunity. This particular Bob is a registered resource proxy. The micropayment system client software on Alice's machine has sent a resource request to Bob, and initiated an authentication session.

5           In the micropayment system universe and on the network are Ted, Reg and other micropayment system supporting servers (such as directory servers, business rules servers, etc. In the framework of the present invention, Bob is also found in this secured zone - and as such possesses extra abilities and features.

10           Bob and Ted are preferably locally connected over a fast connection to reduce throughput between them. Additional potential overhead that might be found in negotiating a large number of session manager authentications is reduced for the same reason. Local connection between session manager components increase scalability options as well as reducing the ultimate "cost-per-click."

15           Resource proxy Bob maintains accounts with multiple resource vendors acting as a universal client.

20           Figure 6 shows existing resource providers. Bob is a client to the many resource-vendor Hal variants that exist in the online world, including e-Commerce schemes ranging from a simple subscription model to Open Market's CSP (Commerce Service Provider). Preferably Bob is equipped to communicate via diverse front-ends supported or enforced by any particular Hal. Bob is a registered user with respect to each of them. Bob and Hal may have an existing relationship. If Bob should encounter a Hal that has an unknown or new e-Commerce scheme, Bob may opt to subscribe. Thus, Alice's requested resource may be fetched by Bob from a previously unknown Hal.

25           Referring to Figure 7, Bob has obtained the resource that Alice wants. Bob has effectively encapsulated any vendor requirements for billing and charges, and is now in possession of Alice's requested resource. Bob functions as a "universal client" to every Hal

and as a "universal server" to every Alice. At this point in the data flow, Bob is ready to service Alice's request for a resource.

During the session manager authentication phase, Alice was recorded by Ted as making the request. Ted now creates a nonce generation event which is used in the debit process.

Stepping back to step three of the session manager authentication, Ted sent Alice a compound message where she read the part destined for her and forwarded the rest, which was encrypted for Bob. The second compound message contained a nonce, or one time key (preferably, a pair of keys) generated by Ted, and such keys are what is sent to Bob and Alice.

Since Bob is directly connected to Ted, the second part of the compound message does not need to be forwarded through Alice. The direct connection between Bob and Ted has the two-fold benefit of reducing overall CPU and bandwidth utilization for all three parties, while increasing security - less information, whether it is encrypted or not, is required to be exposed to the public wire.

The data flow at this stage follows the pattern of Figure 8. Bob has a resource for Alice. When Ted is satisfied that Alice is who she claims to be pursuant to the session manager function, Ted sends Alice a decryption key (1) and its mate to Bob (2). Bob encrypts the resource with his encryption key, sends the encrypted resource to Alice (3) where she can decrypt it with her decryption key. Since a nonce was generated, no one but the intended recipient can obtain the resource in this session, and Alice's acceptance and usage of key provides proof of delivery. The nonce generation event has served its purpose and Ted will decrement the available nonce generation events reserved in Alice's account.

Referring now to Figure 9, the back-office processes required to facilitate transaction processing via the present platform are detailed.

There are two types of transactions within this framework: real-time transactions based on nonce generation events, discussed above, and back-end transaction processing, where user credit instruments are charged and resource vendors are remunerated.

5 The backoffice and accounting services reside apart from the core net-side nonce generation event based transactional activity and across a protected gateway. The backoffice and accounting services layer helps to form the accounting foundation integral to, and found within, any corporate entity.

10 The backoffice and accounting services layer is where client and vendor accounts are processed and where the purchase orders and invoices get entered and fulfilled. The back office and accounting services layer is where statements and checks are printed and posted. The business model resembling the back office in activity and intent from this vantage point, and the view of the National Automated Clearing House Association ("NACHA"), is often described as mail-order/telephone order ("MOTO"). In a typical MOTO system, customer orders are placed via telephone (for the most part) and accepted without the customer's signature, and then charged with central terminal servers.

15 It is important to note, however, that the back end of the preferred embodiment bears a distinct kinship to a service provider's revenue model as well. The user base is asked to pay up front for services which the micropayment system promises to provide at a later time. For example, the nonce generation events may be sold in quantities corresponding to twenty  
20 United States dollars-(US\$20). The subscription agreement between the user and the company providing the micropayment system provides that when the user's supply of nonce generation events gets low enough, the Company is authorized to replenish the user's supply of nonce generation events without the user's needing to intervene.

25 The replenishing debit accounts function is carried out on one or more terminal servers, running clearing software and linked to an external clearing body by a modem and telephone line (or a dedicated) communications link. The external clearing body may be a NACHA representative, credit card company, bank or a national financial non-bank, such as

ATT Capital, GE Capital Services, etc. The back-end transaction processing may be, in general, carried out in different ways with different parties. Preferably the processing system can select parties and processing methods which are advantageous for a given transaction.

5 Alice's fiscal instrument is charged, and upon a successful transaction, she is provided a usable online micropayment system account. Under the subscription agreement, the amount charged will not exceed US\$20.00 and will not be less than a lower limit based on costs enforced by the external clearing body.

10 In order to perform micro-currency transactions without incurring the prepayment costs and the associated risks that come from brokering a transaction, the system utilizes debit accounts. A debit account stores a previously negotiated amount charged against a users credit card or other fiscal instrument. This is sometimes called "pay-to-play" and is functionally similar to the familiar automated teller machine (ATM) paradigm.

15 As mentioned above, the back-end transaction processing can be carried out in a number of ways. Preferably, the various different options for carrying out back-end transaction processing are assembled in a modular layer. One clearing system may prove useful at any single time, but whenever another proves to be more advantageous for any reason (*e.g.*, better rates, partnership arrangements, etc.), the more advantageous system can be adopted without disrupting the rest of the structure.

20 In a preferred procedure for replenishing debit accounts, Ted will determine when Alice has reached a previously agreed upon lower threshold. At that time, Ted will send a message through the secure gateway to a local terminal server. The terminal software will negotiate via modem or leased line connection an authorized charge against Alice's fiscal instrument. Upon a successful clearing transaction, an "ok" status is sent back through the secure gateway to Ted. The process for replenishing debit accounts is similar to the process  
25 for initially charging the debit accounts.

Referring to Figure 10, a basic overview of a micropayment transaction will now be discussed.

1. A user/buyer wants to obtain a resource (article, image, sound, etc.) from an Internet merchant/vendor.
- 5 2. The merchant/vendor requires proof of subscription (either to the merchant's services, or to the merchant's choice of e-Commerce vendor) before the resources will be delivered.
3. The user/buyer is not a subscriber and chooses not to subscribe at this time, but would still like to obtain the resource.
- 10 4. The micropayment client software residing on the user/buyer's personal computer senses the subscription request and offers to obtain the resource for the user/buyer.
5. If the user/buyer chooses to have the micropayment client handle the transaction, a message is sent to the micropayment servers indicating this.
- 15 6. The micropayment server uses it's own subscription to the merchant/vendor to obtain the resource
7. The merchant/vendor recognizes the micropayment server as a subscriber and delivers the resource to the micropayment server.
- 20 8. The micropayment server then delivers the resource to the user/buyer.

The following is a description of the back office procedures utilized by a preferred embodiment of the present invention. As with any company that accepts credit cards for payments, the pieces required to process transactions include a merchant account, a terminal server (such as a card reader), a modem link, and access to a clearing company.

25 Several layers to the credit card payment processing hierarchy are beyond the scope of a simple back-office process. These include:

1. Issuing bank (of the credit card);
2. Interchange access (Visa, MasterCard, AMEX differences, etc.); and

3. Processor (National Automated Clearing House Association representative company).

The complexities of these structures are all masked with traditional terminal server software and hardware issued by an Independent Sales Office (ISO) for a group of national processors.

5           A number of web vendors offer credit-card payment processing services for conducting a transaction on the Internet. Such companies include WebMall, USWeb, Octagon, and CyberCash, etc. Services such companies provide range from the set-up of a merchant account on an organization's behalf to performing the entire online transaction from the company.

10           A preferred micropayment process of the invention does not require online Internet transactions. The micropayment back-office activities are akin to a service organization such AOL, MSN, UUNet, etc. in that the buyer is asked periodically to pre-pay for services that will be rendered. No Internet connection is required for the transaction to transpire, the user need not be online at the time, and the transaction does not occur on the Web. This type of  
15 transaction process is regarded by NACHA as a mail order/telephone order or MOTO transaction because the credit card itself is never physically present when a transaction is processed.

          An Internet service such as the preferred micropayment system does not require an Internet transaction. In fact, it is part of the inherent security and ease of use of the present  
20 invention that the transactional activity occurs offline. The CPU and bandwidth requirements of securing an online transaction are completely removed.

Figure 11 illustrates micropayment system backoffice activity.

1. A micropayment terminal server or other point of sale (POS) device receives a charge request for User X.

2. The terminal server looks up User X in an accounts database and gets the information, "Alice User, CC# 1234 4567 8910, expiration 0999."
3. The terminal server then dials into it's credit card processor and requests a US\$20.00 charge against Alice User's credit card, passing the information ("Alice User, CC# 1234 4567 8910, expiration 0999") it just received from the accounts database.
4. The credit card processor returns a status (either "OK" or "Unable").
5. The terminal server passes only the status of User X back to the secured gateway and the micropayment online servers beyond.

10 If the status were "OK," then the credit card processor debit the cardholders account by US\$20.00 and credits the micropayment merchant account the same US\$20.00. This can be performed in a batch process where many requests for credit card clearing are queued until an appropriate time, or performed at the time of request.

15 Figures 12A-C comprise an exemplary form for creating a merchant account. Though the costs and charges vary, they are roughly as follows:

Application fee:	US\$135.00
Clearing charges:	US\$0.30
Clearing rate:	1.75%.
Card not present:	.75%

20 Note that there is an approximate .75% premium for MOTO (Card not present) transactions.

Micropayment transactions are conducted at the request of multiple buyers. Nonce generating events are issued to users for purchasing resources from multiple merchant/vendors.

25 Periodically, a "transaction dump" or raw data from the Internet is processed, where a measure of used nonce generating events is sent through the secured gateway destined for the



accounting services. Accounting services will receive this raw data and calculate an aggregate yield based on the accumulated usage of a merchant/vendor's resources. No individual buyer's information is kept in the online space or found in the raw data -- such information is not required to remunerate merchant/vendors.

5           As a hypothetical example, suppose 100 users have obtained a news story from vendor "X" over a set period, at an individual cost of US\$0.50 per article. Over this same period, suppose 150 users have played "Doom" for US\$0.25 per play at the website of vendor "Y." In this example, there were 250 unique transactions. Each merchant/vendor is spared the effort of negotiating each transaction, and tracking each user for the low monetary sum each  
10       resource is valued. The data for this period would define US\$50.00 associated with vendor "X" and US\$37.50 associated with vendor "Y."

          Referring to Figure 13, the preferred micropayment process of the invention aggregates small individual purchases into one larger accumulated value. This value is further processed through accounting services to yield a commission for performing these services.  
15       The remaining cash value is processed and a check is issued to each respective merchant/vendor at pre-defined intervals (monthly, bi-weekly, etc.) in one lump sum (as opposed to 250 separate checks of less than a dollar apiece). This is true for every vendor.

          Benefits for user/buyers in this model come from the fact that none of their purchasing dollars are tied to a single merchant/vendor. Their ability to spend nonce generating events  
20       freely allows for more "impulse spending" as well, which also benefits merchant/vendors.

          A particularly preferred embodiment of the intermediation process of the invention for the purchase of digital content from a merchant by a purchaser over the Internet is described below.

          In the preferred embodiment, both the merchant and the purchaser are subscribers to  
25       an automatically-invoked intermediation service which provides facilities for carrying out the process of the invention. In particular, the intermediation service provides a trust server and a

proxy content server. The trust server and the proxy content server can separately access the Internet and can be separately accessed via the Internet. In addition, the trust server and the proxy content server of the intermediation service are interconnected by a private digital communications network separate from the Internet.

5           A preferred arrangement for inter-connecting subscribing purchasers, subscribing merchants, and components of a transaction processing site for the preferred intermediation service is illustrated schematically in Figure 14. The preferred intermediation service employs a modular and distributed arrangement involving a transaction queue for transaction  
10           processing by servers at the transaction processing site, which provides for scalability and work-load balancing by adding additional servers.

Turning now to Figure 14, a plurality of personal computers 300 of buyers who subscribe to the intermediation service, a plurality of web servers 302 of merchants who subscribe to the intermediation service, and a transaction processing site 304 are interconnected by the Internet digital communications network 306. The transaction  
15           processing site 304 includes a plurality of servers 310-330 among which various tasks of transaction processing for the intermediation service are distributed. A core group of the servers 310-322 at the transaction processing site 304 are interconnected by a private transaction-queue interconnection network 332 which facilitates distribution of the transaction processing tasks among the servers of the core group 310-322 and permits additional servers  
20           324 be added to the core group for scaling and work-load balancing. As an example of the distribution of the transaction-processing tasks among the servers of the core group, a banker/membership server 310 may manipulate a subscribing purchaser accounts database; a resource rules database server 312 may manipulate a master copy of a resource-rules database for the service, a trust server 314 may perform purchaser account verification; a supervisor  
25           server 316 may serve decryption keys for decrypting purchased content and order-confirmation messages; a proxy content server 318 may retrieve purchased content from subscribing merchant sites and, if appropriate, parses the content to identify and retrieve software objects embedded in the purchased context; an account server 320 handles the initial formation of new accounts and account maintenance; and an account replenishment server 322

handles replenishment of subscribing purchaser accounts. The account replenishment server 322 can communicate with a credit-card processor 332 of a financial institution via a channel 334 separate from the Internet. A master database server 326 logs transactions processed by the core group and stores the subscribing purchaser accounts database and the master copy of the resource-rules database and, in conjunction with an account database server 324, maintains financial account data such as credit card numbers of subscribing purchasers. An accounting system server 330 may handle disbursements to subscribing merchants and a data mining system 328 may collect statistical data concerning use of the transaction processing site. Communication between the transaction processing site 304 and the Internet is mediated by a firewall system 340 which controls access to the servers of the site.

The preferred intermediation service of the invention maintains a subscriber-purchaser accounts database and a subscriber-merchant accounts database, both of which can be accessed by the trust server and the proxy content server not via the Internet. The subscriber-purchaser accounts database includes for each subscribing purchaser, a purchaser account identification number, cryptographic information for communicating with the subscribing purchaser, a purchaser account balance, and information for replenishing the purchaser's account. Table I below sets forth the information maintained for each subscribing purchaser in the subscriber-purchaser accounts database.

Table I  
Subscriber Purchaser Accounts Database

Key	Name	Type	Description
•	UserID	NUM(10)	ID of the purchaser
	PreviousSecret	NUM(10)	Previous shared secret
	Secret	NUM(10)	Secret User shares with the trust server
	NextSecret	NUM(10)	Next secret for encryption
	ReplenishAmount	NUM(10)	Amount for automatic replenishment
	ReplenishInProgress	NUM(10)	If TRUE, additional request for replenish won't occur
	AccountStatus	NUM(10)	Used to determine if account is active, pending delete or withdrawal, etc.)
	ReplenishType	NUM(10)	Describes whether manual/automatic replenishment is set.
	HighReplenish	NUM(10)	The value of balance for sending replenish for this purchaser in \$0.0001
	Balance	NUM(10)	Balance of the purchaser account in units of \$0.0001

The subscriber-merchant accounts database includes information encoding universal resource locator ("URL") data identifying one or more restricted-access ports at each subscribing merchant site on the network, and, for each such restricted-access port, information encoding an access fee for accessing content by way of the restricted-access port and a password for obtaining access to content by way of the restricted-access port.

A subscribing purchaser will generally communicate over the Internet using a personal computer running an Internet browser program and making use of the services of a commercial Internet service provider ("ISP"). Subscription to the preferred intermediation service of the invention is generally initiated "online" over the Internet, with the new subscriber accessing a Web site of the intermediation service. Referring to Figure 15, the preferred intermediation service downloads a subscription application screen 400 in hypertext markup language ("HTML") format for display on the display screen of the personal computer of the new subscriber. The subscription application screen 400 includes HTML data-entry fields labeled to prompt for entry of the new subscribing purchaser's name 402 and billing address 404, including e-mail address.

The preferred intermediation service maintains a purchaser account for each subscribing purchaser against which charges for purchases made by the purchaser using the intermediation service are applied. The purchaser account of a new purchaser is opened with an initial deposit which is withdrawn from another financial account of the new subscribing purchaser, such as a credit-card account maintained with a bank or other financial institution. The subscription application screen 400 includes HTML data-entry fields labeled to prompt for entry of billing information 406 to be registered with the intermediation service, including card type, card number, and expiration date. The subscription application screen 400 also includes HTML data-entry fields labeled to prompt for entry of purchaser account replenishment information 408, including the amount of an initial deposit in the purchaser account of the new subscribing purchaser. When the balance in a purchaser account maintained by the preferred intermediation service falls below a "replenishment threshold" value, the purchaser account is replenished by making a withdrawal of a replenishment amount

from the credit-card or other financial account of the subscribing purchaser registered with the intermediation service and crediting the purchaser account by the replenishment amount withdrawn. The replenishment information 408 prompted for in the subscription application screen 400 includes a replenishment threshold value, a replenishment amount, and a selection of whether the replenishment is to be carried out automatically or manually by the subscribing purchaser.

Upon transmission of the subscription information prompted for by the subscription application form 400 to a transaction processing site of the preferred intermediation service and verification of the billing information by withdrawal of the initial deposit from the financial account of the new subscribing purchaser, a subscription confirmation screen 410 illustrated in Figure 16 is downloaded in HTML format over the Internet from the transaction processing site to the personal computer of the new subscribing purchaser for display on the personal computer under the control of the browser program. The subscription confirmation screen 410 indicates that a subscribing purchaser account has been successfully established and identifies the purchaser account number. The HTML instructions which specify the subscription confirmation screen 410 painted by the browser on the display screen of the personal computer of the new subscribing purchaser define a labeled control area 412 which carries the label: "click here to download redirection and authentication control program." In accordance with the HTML instructions specifying the subscription confirmation screen 410, the browser can detect when a user executes a "mouse click" when the cursor of the display screen is positioned within the labeled control area. In response to detecting such a mouse click, the browser program transmits a control action message over the Internet to the transaction processing site of the intermediation service which indicates that a mouse click occurred in the labeled control area 412. Upon receipt of the control action message from the subscribing purchaser's computer at the transaction processing site of the intermediation service, a redirection and authentication control program is downloaded over the Internet from the transaction processing site and installed in the personal computer of the new subscribing purchaser.

The redirection and authentication control program runs on the personal computer of each subscribing purchaser of the preferred automatically invoked intermediation service and locally monitors Internet communication activity information generated by the Internet browser program running on the personal computer. The redirection and authentication control program can monitor Internet communication activity generated by the browser program using the application programming interface "API" of the browser program. For example, the redirection and authentication control program can monitor communication activity information generated by a "Netscape Navigator" browser program by way of the "DDE API" interface of the Navigator program and can monitor communication activity information generated by a "Microsoft Internet Explorer" browser program by way of the "COM" interface of the Internet Explorer program.

In order to accomplish URL interception from the Netscape Navigator browser, for example, the following DDE interface calls may be used:

- DdeConnect, DdeDisconnect -- Establishes/closes a DDE connection to the browser. One DDE connection is all that is necessary to monitor all Navigator browser windows.
- WWW\_RegisterProtocol, WWW\_UnRegisterProtocol (DdeConversation) -- allows the redirection and authentication control program to register the HTTP, FTP, and any other Internet protocols. This allows the control program to take control every time a URL is requested of the browser.
- WWW\_ViewDocFile, WWW\_WindowChange, DdeFreeStringHandle, DdeClientTransaction, DdeCreateStringHandle, DdeNameService, DdeQueryString, DdeUnaccessData, DdeFreeDataHandle -- maintenance of DDE functions, that altogether allow for the URL interception to take place.

OpenURL, which is not a DDE operation may be used to process a URL request. This call is used for two purposes: (1) to return control to the browser for URL requests for which there are no resource rules database entries; and (2) to instruct the browser to display a cached resource retrieved by the control program via the intermediation service.

The redirection and authentication control program installed in the personal computer of each subscribing purchaser to the preferred intermediation service includes a resource rules database for identifying Internet communication activity information generated by the browser program running on the personal computer with respect to accessing resources available by way of restricted-access ports of network sites of subscribing merchants to the intermediation service. For each of at least a subset of the restricted access ports at subscribing merchant sites identified in the subscriber-merchant accounts database, the resource rules database of the redirection and authentication control program installed in a given subscribing purchaser's personal computer includes a data structure referred to as a "rule" which functions as a scripting language to permit search criteria specified in the rule to be applied to URL's or other communication activity information generated by the Internet browser program running on the computer. For example, a rule could be used to test a URL for the presence of a particular keyword or a hostname to identify a restricted-access port at a subscribing merchant's site. In addition, rules include information for determining how much is to be charged for access to the resource in the restricted access port and for how long access to the resource is to be permitted once permission to access has been purchased.

A master resource rules database is maintained at the transaction processing site of the preferred intermediation service for updating the local resource rules databases in the personal computers of the subscribing purchasers from time to time. Subscribing purchasers may maintain copies of the full master resource rules database or may maintain a copy of the resource rules database for only a subset of the restricted-access ports identified in the master resource rules database. Such a subset might, for example, be limited to sites suitable for access by children, or, for purposes of limiting the size of the resource rules database in the personal computer of subscribing purchasers, to sites with content in a particular language.

The master copy of the resource rules database is structured as a structured query language ("SQL") database. An entry in the master copy of the resource rules database takes the form of an SQL table row. Product, fee schedule, and term information used to form the entry in the database is obtained from the subscribing merchant who is to provide the product. For distribution to subscribing purchaser sites, a "flat-file" version of the master copy of the

resource rules database is prepared at the transaction processing site, which is then compressed using a conventional data compression algorithm. The compressed flat-file version of the resource rules database is distributed to new subscribing purchaser sites along with the redirection and authentication control program. To maintain the local versions of the resource rules database current at subscribing purchaser sites, the redirection and authentication control program queries the transaction processing site upon initialization of each Internet connection and every twenty four hours for the date of the current version of the master copy of the resource rules database. If the master copy of the resource rules database at the transaction processing site is more recent than the local copy maintained at the subscribing purchaser site, the redirection and authentication control program downloads a copy of the most recent resource rules database in the compressed file format, decompresses the downloaded database file, and updates the copy of the database maintained at the purchaser site. Updated purchase terms are generally distributed throughout the intermediation service within forty-eight hours.

The following Table II gives the structure of the resource rules database.

**Table II**  
**Resource Rules Database**

**Host Table**

Key	Name	Type	Description
•	HostName	STR(256)	Hostname of the URL
	HostID	NUM(10)	ID associated with this hostname

**RuleLookup Table**

Key	Name	Type	Description
•	HostID	NUM(10)	ID associated with hostname
	RuleID	NUM(10)	ID associated with rule belonging to the HostID

**Rule Table**

Key	Name	Type	Description
•	RuleID	NUM(10)	ID associated with a rule
	Rule	CHAR(512)	Rule itself. A locator string in a logical expression.



RuleDetail Table

Key	Name	Type	Description
•	RuleID	NUM(10)	ID associated with a rule
	Type	NUM(1)	Type of receipt that will be generated for this rule (URL    Rule ID)
	Duration	NUM(10)	Duration of content purchased under this rule in minutes
	RetailPrice	NUM(10)	Price of content purchased under this rule in cents
	CostOfGoods	NUM(10)	Amount due vender for this item
	ExpirationDate	STR(12)	Date when this rule becomes invalid
	Description	STR(255)	Expression that describes the rule to the user
	VendorID	NUM(10)	Identification of the vendor

The redirection and authentication control program running on the personal computer of a subscribing purchaser functions to intercept automatically requests to access a target resource at a restricted-access port of an Internet site of one of the subscribing merchants, to notify the subscribing purchaser that access to such resource may be had under certain conditions including payment of an access fee, and, if the subscribing purchaser chooses to accept the conditions, to redirect the request for access to the transaction processing site of the intermediation service for charging the subscribing purchaser's account the amount of the access fee and fulfilling the request for access to the target resource. The functioning of the redirection and authentication control program of the preferred intermediation service from the perspective of a subscribing purchaser is described below in terms of a hypothetical example involving accessing content at the Internet site of an online financial newspaper.

When a subscribing purchaser desires to browse the Internet, he or she launches a browser program on his or her personal computer and establishes communication with an Internet service provider. The redirection and authentication control program of the preferred intermediation service is launched automatically upon the launching of the browser program. Each time the subscribing purchaser navigates to a new Internet site, the browser program generates a URL which identifies the site on the Internet. Transparently to the subscribing purchaser, the redirection and authentication control program monitors each URL generated by the browser program before the URL is transmitted by the browser program from the personal computer and determines if the URL corresponds to a restricted-access port of a subscribing merchant identified in the resource rules database of the control program.

Consider the cases of one person who has an account with the intermediation service for carrying out the preferred embodiment of the subject invention and another person who does not have such an account, both of whom desire to access an article in the online financial newspaper over the Internet. Both the subscriber and the nonsubscriber to the intermediation service would typically first navigate to a publicly accessible port of the Internet site of the online newspaper to view a newspaper contents screen 414 which would describe the contents of the newspaper and contain links 416 to certain articles and financial data published in newspaper, as illustrated in Figure 17. The articles and financial data, however, would not be accessible to the general public, but would be available only to subscribers of the online newspaper. Thus, if the person who was not a subscriber to the intermediation service attempted to navigate to one of the articles identified in the publicly accessible contents screen 414 of Figure 17, the person would receive a newspaper subscription screen 416 calling for entry of a newspaper subscription user name and password as a condition to access the article, as shown in Figure 18. A subscribing purchaser to the preferred intermediation service, upon attempting to navigate to the same article identified in the publicly accessible newspaper contents screen 414 of Figure 17, would be shown an intermediation-service pop-up window 422 offering the subscribing purchaser the option of accessing the nonpublicly accessible contents of the online newspaper for an access fee and an access time specified in the pop-up window, as illustrated in Figure 19. The intermediation-service pop-up window would generally appear practically instantaneously after the subscribing purchaser attempted to access the non-publicly accessible article, since the redirection and authentication control program of the intermediation service running locally on the subscribing purchase's personal computer would have intercepted the URL generated by the browser program to access the article and would have determined by searching the resource rules database maintained locally on the personal computer that the URL corresponded to a restricted-access port of subscribing merchant to the intermediation service - the online financial newspaper. As a result, the redirection and authentication control program would block transmission of the URL and, using access fee and access time data retrieved locally from the resource rules database, generate the intermediation service pop-up window 422.

As shown in Figure 19, the intermediation-service pop-up window 422 generated by the redirection and authentication control program includes two "push-button" control areas 426 and 428 respectively labeled "OK" and "cancel" to prompt for proceeding with the access under the access fee and access time conditions 424 specified in the pop-up window or termination the access process under the intermediation service. If the "cancel" push-button control area 428 is selected, the browser is permitted to transmit the blocked URL and the newspaper subscription screen 418 appears as shown in Figure 18. If the "OK" push-button control area 426 is selected, the request for access to the restricted-access port of the online newspaper is redirected by the redirection and authentication control program over the Internet to the transaction processing site of the preferred intermediation service, as discussed below.

If the subscribing purchaser elects to proceed with the requested access under the conditions specified in the intermediation-service pop-up window 422 by executing a mouse click with the cursor positioned on the push-button control area 426 labeled "OK" on the pop-up window 422, a six-step authentication and fulfillment procedure in accordance with the preferred intermediation process is initiated to authenticate and fulfill the requested access.

In the first step of the authentication and fulfillment procedure of the preferred intermediation process, the redirection and authentication program running on the subscribing purchaser's personal computer forms a URL request data object which is composed of three fields for encoding respectively: (1) the rule identification number - designated "Rule ID" in Table II above - of the rule in the resource rules database which matched the URL generated by the browser program in connection with attempting to access a target resource by way of the restricted-access port of the Internet site of a subscribing merchant and led to the presentation of the intermediation-service pop-up window, (2) the type of the rule, which specifies the type of receipt which will be generated for the rule, and (3) the URL of the target resource accessible by way of the restricted-access port in question.

For authentication purposes, the local redirection and authentication control program maintains a ten digit number denoted " $S_A$ " referred to as the "account secret" which

can be used as an encryption and decryption key in an encryption/decryption procedure. The value of the account secret is updated after each transaction to access a target resource by way of a restricted-access port at an Internet site of a subscribing merchant. As may be seen in Table I, values for a previous account secret, the current account secret, and a next account secret are maintained for the account of each subscribing purchaser in the subscriber-purchaser accounts database maintained at the transaction processing site of the preferred intermediation service.

Also for authentication purposes, a transaction random number is generated by the redirection and authentication control program for each transaction to access a target resource by way of a restricted-access port at an Internet site of a subscribing merchant.

After generation of the transaction random number, the redirection and authentication control program forms a first-step-identifier, random-number augmented data object composed of a first-step identifier code number designated  $\alpha_1$  and the transaction random number. The first-step-identifier, random-number augmented data object is then encrypted by the redirection and authentication control program using a conventional data encryption procedure with the current account secret number as the encryption key. The encryption procedure used permits the encrypted data object to be decrypted with the same key value.

A redirected purchase-request message is then transmitted over the Internet from the personal computer of the subscribing purchaser by the redirection and authentication control program to the proxy content server of the preferred intermediation service. The redirected purchase-request message is composed of the purchaser account number, a version identification number for the intermediation procedure, the first step identifier code number  $\alpha_1$ , the URL request data object, and the encrypted first-step-identifier, random-number-augmented data object. Transmission of the redirected purchase-request message to the proxy content server concludes the first step of the authentication and fulfillment procedure of the preferred intermediation process.

In the second step of the authentication and fulfillment procedure of the preferred intermediation process, the proxy content server receives the redirected purchase-request message from the personal computer of the subscribing purchaser and checks the first-step-identifier code number  $\alpha_1$  and the version identification number included in the purchase-request message and generates an appropriate error message and terminates the authentication and fulfillment procedure if either is not recognized. If both the first-step-identifier code number  $\alpha_1$ , and the version identification code in the redirected purchase request message are recognized by the proxy content server, the proxy content server retransmits the redirected purchase request message without change to the trust server of the preferred intermediation service over the private network interconnecting the proxy content server and the trust server, thereby concluding the second step of the authentication and fulfillment procedure.

In the third step of the authentication and fulfillment procedure carried out by the preferred intermediation service, the trust server receives the redirected purchase-request message and extracts the rule identification number and the URL for the target resource from the URL request data object included in the purchase-request message. The trust server checks the validity of the redirected purchase request by determining whether the rule identification number and the URL of the target resource correspond to one another in the master resource rules database maintained at the transaction processing site of the preferred intermediation service. If the rule identification number and the URL of the target resource correspond in the master resource rules database, the authentication and fulfillment procedure is permitted to proceed, otherwise the procedure is terminated and an appropriate error message is generated. The first-step-identifier code  $\alpha_1$  is again extracted from the redirected purchase-request message and checked. If the code is not recognized, the authentication and fulfillment procedure is terminated and an appropriate error message issued.

If the authentication and fulfillment procedure is permitted to proceed, a resource encryption key is generated at the trust server by the following procedure. First, two random numbers are generated and then combined to form a double-random-number data object. The double random-number data object is then processed according to a known cryptographic message digest algorithm known as the "SHA1" secure hash algorithm. The SHA1 secure

hash algorithm is described in the following publications: "Secure Hash Standard," National Institute of Standards and Technology, TIPS Publication 180, May 1993 and "SHA-1, Announcement of Weakness in the Secure Hash Standard," National Institute of Standards and Technology, May 1994. The result of applying the SHA1 secure hash algorithm to the double-random-number data object is taken as the resource encryption key.

Next, the purchaser account number and the encrypted first-step-identifier, random-number-augmented data object are extracted from the redirected purchase-request message at the trust server. Using the purchaser account number, the current account secret  $S_A$  and the previous account secret  $S_{Ap}$  are retrieved from the subscriber-purchaser accounts database maintained at the transaction processing site of the preferred intermediation service. If the purchaser account number is unrecognized, the authentication and fulfillment procedure is terminated and an appropriate error message generated. A decryption algorithm using the account secret as decryption key is then applied to the encrypted first-step-identifier, random-number-augmented data object from the redirected purchase-order message and the result checked to determine if the decryption was successful by determining if the first step identifier code number  $\alpha_1$  was extracted. If the first decryption attempt was not successful, a second decryption attempt is made by the applying the decryption algorithm to the encrypted first-step-identifier, random-number augmented data object using the previous account secret  $S_{Ap}$  as decryption key, in case the redirected purchase-request message transmitted by the subscribing purchaser's computer had been delayed. The result of the second decryption attempt is checked as before to determine if the decryption was successful by determining if the first step identifier code number  $\alpha_1$  was extracted. If the second decryption attempt was not successful, the authentication and fulfillment procedure is terminated by the trust server and an appropriate error message issued, in that the identity of the subscribing purchaser whose purchaser account number was included in the redirected purchase-request message was not confirmed.

If either of the two decryption attempts was successful, the authentication and fulfillment procedure is permitted to proceed by the trust server. In the case in which the second decryption attempt using the previous account secret  $S_{Ap}$  as decryption key was the

successful one, a working value of the current account secret for the account in the trust server is set equal to the value of the previous account secret  $S_{Ap}$ . Also in the case in which the second decryption attempt was successful, a working value of the transaction random number in the trust server is set equal to the value of the random number extracted from the decrypted encrypted first-step-identifier, random-number augmented data object, which, in that case, represented the transaction random number of the previous transaction.

Subsequently in the third step of the authentication and fulfillment procedure, a verified-account-identity purchase-request message is transmitted from the trust server to the proxy content server over the private network interconnecting the trust server and the proxy account server. The verified-account-identity purchase-request message includes data encoding the version identification number for the intermediation procedure taken from the redirected purchase-request message previously forwarded to the trust server from the proxy content server, a third step identifier code number  $\alpha_3$ , the resource encryption key generated at the trust server, and the URL for the target resource taken from the redirected purchase-request message.

After transmission of the verified-account-identity purchase-request message by the trust server, a composite session key is composed as a sum of the resource encryption key included in the verified-account-identity purchase request message and a locally-computable key augmentation value. The locally-computable key augmentation value is computed by applying the SHA1 secure hash algorithm three times in succession. First, the SHA1 secure hash algorithm is applied to a first composite data object composed of the working values of the transaction random number originally generated by the redirection and authentication control program running on the subscribing purchaser's personal computer and the current account secret  $S_A$  in the trust server to obtain a first hash value. The first hash value is combined with the working values of the transaction random number and the current account secret to form a second composite data object. The SHA1 secure hash function is then applied to the second composite data object to obtain a second hash value. The second hash value is then combined with the working values of the transaction random number and the current account secret to form a third composite data object. The SHA1 secure hash function

is then applied to the third composite data object to yield a third hash value which serves as the locally-computable key augmentation value. The locally-computable key augmentation value can also be computed locally by the redirection and authentication control program in the personal computer of the subscribing purchaser, since the values of the transaction random  
5 number and the current account secret are available locally to the redirection and authentication control program.

In the fourth step of the authentication and fulfillment procedure, the URL of the target resource is extracted from the verified-account-identity purchase-request message at the proxy content server. The URL of the target resource is used as a pointer to the resource  
10 rules data base to extract a vendor identification number. The vendor identification number in turn is used to extract from the subscriber-merchant accounts database a password for accessing the target resource by way of the restricted-access port of the subscribing merchant. Using the URL for the target resource and the password for obtaining access to the target resource by way of the restricted-access port of the Internet site of the subscribing merchant,  
15 the target resource is accessed and transmitted over the Internet to the proxy content server at the transaction processing site of the preferred intermediation service.

After the proxy content server receives the target resource, the target resource is combined with a fourth-step-identifier code number  $\alpha_4$  to form a step-labeled target-resource composite data object. The step-labelled target-resource composite data object so formed is  
20 then encrypted with an encryption algorithm which employs the resource encryption key extracted from the verified-account-identity purchase-request-message as the encryption key for the algorithm.

To conclude the fourth step of the authentication and fulfillment procedure, an encrypted-target-resource delivery message is transmitted over the Internet from the proxy  
25 content server to the personal computer of the subscribing purchaser who originally attempted to access the target resource. The encrypted-target-resource delivery message includes data encoding the version identification number for the intermediation procedure, the fourth step identifier code number  $\alpha_4$ , and the encrypted step-labelled target-resource data object.



For the fifth step of the authentication and fulfillment procedure, the locally-computable key augmentation value previously computed at the trust server in the third step of the procedure is recomputed independently by the redirection and authentication control program running on the personal computer of the subscribing purchaser. The final key augmentation value and the intermediate hash values obtained in computing the final key augmentation value should be identical whether computed at the trust server or at the subscribing purchaser's personal computer, since the same procedure involving applying the SHA1 secure hash algorithm three times in succession to successive composite data objects formed from the transaction random number, the current account secret, and prior hash values can be followed in both cases and the values for the transaction random number and the current account secret are the same.

As discussed below, a receipt data object is generated in the sixth step of the authentication and fulfillment procedure for each transaction in which access to a target resource is obtained by means of the preferred intermediation service and transmitted to the personal computer of the subscribing purchaser. The elements of the receipt data object are specified in Table III below:

Table III  
Receipt Data Object

Key	Name	Type	Description
•	RuleID	NUM(10)	ID associated with a rule.
	URL	STR(1024)	Include this with receipt if the URL is required by the rule type.
	LocalExpirationDate	DATE	Used locally to determine if this content is paid for.
	ServerExpirationDate	DATE	Proves to the server that this content is paid for.
	KeyID	NUM(10)	A pointer to an array of keys maintained in the trust server; Indicates which key was used in the hash.
	ReceiptHash	STR(1024)	Indicates the resultant of the hash.
	User ID	NUM(10)	Purchaser account number

The receipt data object may be presented to the transaction processing site of the intermediation service to enable the subscribing purchaser to obtain multiple accesses to the target resource - say, over a fixed period of time established by the rule - without incurring multiple charges. With respect to the present discussion of the fifth step of the authentication and fulfillment procedure, it should be borne in mind that the redirection and authentication control program running on the subscribing purchaser's personal computer may or may not have a receipt data object at the time of a given instance of the fifth step of the authentication and fulfillment procedure, depending on whether the transaction had previously progressed to a stage at which a receipt data object was generated and transmitted to the subscribing purchaser's personal computer.

Whether or not the redirection and control program has a receipt data object in a particular instance of a fifth step of the authentication and fulfillment procedure for a given transaction, the redirection and authentication control program forms a step-labeled receipt indicator composite data object. In the case the redirection and control program has previously received a receipt data object for the transaction, the step-labeled receipt-indicator composite data object is formed by combining the fifth-step identifier code number  $\alpha_5$  with the following data elements from the receipt data object: RuleID, ServerExpirationDate, UserID, KeyID, ReceiptHash, and, if appropriate to the rule type, the URL of the target resource. In the case the redirection and control program has not previously received a receipt data object for the transaction, the step-labeled receipt-indicator data object is formed by combining the fifth-step indicator code number with code indicating that no receipt data object is present. In either case, the step-labeled receipt indicator composite data object is then encrypted with an encryption algorithm using as the encryption key the second hash value obtained as the result of the second of the three successive applications of the SHA1 secure hash algorithm made in connection with the calculation of the locally-computable key augmentation value.

A resource-decryption-key request message is assembled by the redirection and authentication control program running on the personal computer of the subscribing purchaser after receiving the encrypted target-resource delivery message from the proxy content server of the preferred intermediation service. The resource-decryption-key request message is

composed of data encoding the purchaser account number, the version identification number of the intermediation procedure, the fifth-step identifier code number  $\alpha$ , and the encrypted step-labeled receipt-indicator composite data object. The resource-decryption-key request message is transmitted from the personal computer of the subscribing purchaser to the trust server of the preferred intermediation service over the Internet to conclude the fifth step of the authentication and fulfillment procedure of the preferred intermediation process.

In the sixth and final step of the authentication and fulfillment procedure of the preferred intermediation process of the invention, a determination is made at the trust server of the intermediation service carrying out the preferred intermediation process in response to the resource-decryption-key request message from the subscribing purchaser's personal computer whether or not to transmit a resource decryption key to the subscribing purchaser, and, if so, whether to charge the subscribing purchaser's account for the access fee in connection with transmitting the resource decryption key. As discussed in more detail below, the determination of whether to charge the subscribing purchaser's account for the access fee involves three test criteria applied with respect to the step-labeled receipt-indicator data object included in the resource-decryption-key request message: (1) does the data object include a receipt data object?; (2) if a receipt data object was included, is it genuine?; and (3) if a receipt data object was included, has the expiration date passed?

First, the encrypted step-labeled receipt-indicator composite data object is decrypted at the trust server using as decryption key the second hash value obtained as the result of the second of the three successive applications of the SHA1 secure hash algorithm made in connection with the calculation of the locally-computable key augmentation value. Extraction of the fifth-step identifier code number  $\alpha$ , from the decrypted step-identified receipt indicator composite data object verifies the identify of the subscribing purchaser specified by the purchaser account number included in the resource-decryption-key request message.

If the identify of the subscribing purchaser specified by the purchaser account number included in the resource-decryption-key request message is verified, the decrypted step-labeled

receipt-indicator composite data object is checked to determine if a receipt data object was included in the data object.

5 If no receipt data object was found to have been included in the step-labeled receipt-indicator composite data object, the subscribing purchaser's account with the intermediation service is charged the amount of the access fee for accessing the target resource.

10 If a receipt data object was found to have been included in the step-labeled receipt-data composite data object, the genuineness of the receipt data object is checked before proceeding. Specifically, the SHA1 secure hash algorithm is applied to a composite data object formed of the following data elements included in the receipt data object: KeyID, RuleID, ServerExpirationDate, UserID, and, if called for by the rule type, the URL of the target resource. If the result of the SHA1 hash function matches the ReceiptHash included in the receipt data object, indicating that the receipt data object is genuine, the authentication and fulfillment procedure proceeds to the date verification step without charging the subscribing purchaser's account. If the result of the SHA1 has function does not match the ReceiptHash in the receipt data object, the receipt data object is not genuine and the subscribing purchaser's account is charged the amount of the access fee. If a receipt data object was found to have been included in the step-labeled receipt-indicator composite data object and the receipt data object was found to be genuine, the server expiration date encoded in the receipt data object is compared to the current date provided by the trust server. If the server expiration date has not been exceeded, no charge is made to the subscribing purchaser's account. If the server expiration date has been exceeded, the subscribing purchaser's account is charged the access fee.

25 If the identity of the subscribing purchaser is verified and either no receipt data object was found to be included in the step-labeled receipt indicator composite data object, or a receipt data object was found to be included in the composite data object and the receipt data object was determined to be genuine, a resource-decryption-key delivery message is assembled at the trust server. The resource-decryption-key delivery message is composed of data-encoding the following data elements: the purchaser account number, the version

identification number of the intermediation procedure, a sixth-step identifier code number  $\alpha_6$ , and an encrypted step-labeled key/receipt-carrier composite data object. The step-labeled key/receipt-carrier composite data object is formed of the sixth-step identifier code number  $\alpha_6$ , the composite session key computed in the third step of the authentication and fulfillment  
5 procedure discussed above, and, a receipt data object incorporating the data elements identified in Table III above. The step-labeled key/receipt-carrier composite data object is then encrypted using an encryption algorithm employing as encryption key the second hash value obtained as the result of the second of the three successive applications of the SHA1 secure hash algorithm made in connection with the calculation of the locally-computable key  
10 augmentation value.

The resource decryption-key delivery message is transmitted from the trust server to the personal computer of the subscribing purchaser over the Internet. After the transmission of the resource-decryption-key delivery message, the record of information specific to the transmission may be cleared from the trust server.

15 After receipt of the resource-decryption-key delivery message at the personal computer of the subscribing purchaser, the redirection and authentication program running on the computer applies a decryption algorithm to the encrypted step-labeled key/receipt carrier composite data object using as decryption key the result of the second of the three successive applications of the SHA1 secure hash algorithm made in connection with the calculations of  
20 the locally-computable key augmentation value. As noted above, the calculation for the locally-computable key augmentation value can be carried out identically on the trust server and locally on the subscribing purchaser's personal computer. Decryption of the encrypted step-labeled key-receipt carrier composite data object enables the redirection and authentication control programs to obtain the value of the composite session key included in  
25 the data object. The resource decryption key may then be obtained locally from the composite session key by subtracting the locally-computable key augmentation value from the composite session key. The resource decryption key may then be used by the redirection and authentication control program to decrypt the encrypted target resource previously transmitted to the personal computer of the subscribing purchaser from the proxy content

server in the fourth step of the authentication and fulfillment procedure of the intermediation process. For example, the subscribing purchaser can peruse an article from the online financial newspaper 429 on the display screen of his or her personal computer, as illustrated in Figure 20.

5           In addition, decryption of the encrypted step-labeled key/receipt carrier composite data object enables the redirection and authentication control program to obtain a receipt data object included in the composite data object. Obtaining the receipt data object permits the subscribing purchaser to access additional content in the online newspaper without further charge until the server expiration date included in the receipt data object is exceeded.

10           Finally, the sixth step of the authentication and fulfillment procedure concludes by updating the account secret at the personal computer of the subscribing purchaser by setting the new account secret equal to the result of the first of the three successive applications of the SHA1 secure hash algorithm made in connection with the calculation of the locally-  
15           computable key augmentation value. Additionally, the account secret values in the subscriber-purchaser accounts database at the transaction processing site are updated by setting the new previous account secret value equal to the old current account secret value and setting the new current account secret value equal to the previously determined first hash value, which was the result of applying the SHA1 secure hash algorithm to the first composite data object composed of the working values of the transaction random number and the current account secret  $S_A$ .

20           The subscribing purchaser may monitor the status of his or her account with the preferred intermediation service by downloading an account maintenance screen 430 for the account from the transaction processing site, as illustrated in Figure 21.

25           It is not intended to limit the present invention to the specific embodiments described above. For example, it is recognized that these and other changes may be made in the intermediation process for network purchases of the invention specifically described herein without departing from the scope and teachings of the instant invention, and it is intended to encompass all other embodiments, alternatives, and modifications consistent with the invention.

## CLAIMS

1. An automatically invoked intermediation process for purchasing content over a digital communications network by subscribing purchasers from subscribing merchants, the intermediation process comprising the steps of:

5 (a) establishing a database of subscriber-purchaser accounts and a database of subscriber-merchant accounts at a central transaction processing site on the digital communications network, the subscriber-merchant accounts database including information encoding resource locator data identifying at least one restricted-access port at each subscribing merchant site on the network and, for each such restricted-access port, information encoding an access fee schedule for accessing  
10 content by way of the restricted-access port and access-restriction-override information for enabling access to content by way of the restricted-access port, and the subscriber-purchaser accounts database including information encoding purchaser site authentication credentials and a purchaser account balance for each subscribing purchaser;

15 (b) at the network site of each subscribing purchaser, establishing a resource rules database including information encoding resource-locator-data identification criteria corresponding to each of at least a subset of the restricted-access ports at subscribing merchant sites identified in the subscriber-merchant accounts database and the access fee schedule for accessing content by way of the  
20 corresponding restricted-access port;

(c) at the network site of each subscribing purchaser, locally monitoring network communication activity information with respect to access to a target network resource generated by a browser program at the subscribing purchaser site and comparing such network communication activity information to the resource-locator-data identification criteria corresponding to restricted-access ports at the network sites  
25 of subscribing merchants in the resource rules database locally maintained at the site of the subscribing purchaser;

(d) in the event network communication activity information pertaining to the target network resource of step (c) matches with the resource-locator-data identification criteria corresponding to a restricted-access port in the resource rules database, retrieving the access fee schedule corresponding to the matched resource-locator-data identification criteria from the resource rules database, displaying an access fee from the access fee schedule for accessing content by way of the restricted access port corresponding to the resource-locator-data identification criteria, and prompting for approval or disapproval of completing the access for the displayed access fee;

(e) upon receipt at the subscribing purchaser site of a user communication responsive to the prompting of step (d) indicating approval of completing the access to content by way of the restricted-access port for the access fee, transmitting a purchase-request message from the subscribing purchaser site to the transaction processing site over the network, the purchase-request message including information encoding purchaser-site authentication credentials and identifying the restricted-access port at the merchant site corresponding to the matched resource-locator-data identification criteria;

(f) upon receipt of the purchase-request message of step (e) at the transaction processing site, determining whether the purchaser-site authentication credentials encoded in the purchase-request message matches with any purchaser-site authentication credentials included in the subscriber-purchaser accounts database and, if such a match is found, transmitting over the network to the restricted-access port of the merchant site a restricted-access-enabling access-request message to download purchased content by way of the restricted-access port to the transaction processing site, the restricted-access-enabling access-request message including access-restriction-override information corresponding to the restricted-access port retrieved from the subscriber-merchant accounts database;

(g) upon receipt of the downloaded purchased content at the transaction processing site from the subscribing-merchant site by way of the restricted-access port responsive to the restricted-access-enabling access-request message of step (f),



encrypting the downloaded purchased content and forwarding the thus encrypted  
purchased content to the subscribing purchaser site over the network;

(h) upon receipt of the encrypted purchased content of step (g) at the  
subscribing purchaser site, transmitting a content-received confirmation message to the  
transaction-processing site by the subscribing purchaser site over the network;

(i) upon receipt of the content-received confirmation message of step  
(h) from the subscribing purchaser site at the transaction processing site, debiting the  
purchaser account balance corresponding to the subscribing purchaser in the  
subscriber-purchaser accounts database by the access fee for accessing purchased  
content by way of the restricted-access port and forwarding a cryptographic key for  
decrypting the encrypted purchased content to the subscribing purchaser site over the  
network; and

(j) upon receipt of the cryptographic key at the subscribing purchaser  
site, decrypting the encrypted purchased content at the purchaser site.

2. The automatically invoked intermediation process according to claim 1 in which the access  
fee schedule corresponding to a restricted-access port in the subscriber-merchant accounts  
database consists of a single access fee for accessing content by way of the restricted-access  
port.

3. The automatically invoked intermediation process according to claim 1 further including  
the steps of parsing the downloaded purchased content at the transaction processing site prior  
to encrypting the purchased content to extract any resource locator data corresponding to  
software objects embedded in the content, retrieving the software objects over the digital  
communications network using the resource locator data, and combining the software objects  
with the purchased content to form a composite purchased-content data object, and in which  
the step of encrypting the downloaded purchased content is carried out by the encrypting the  
composite purchased-content data object.

1 4. The automatically invoked intermediation process according to claim 3 in which the  
2 downloaded purchased content is a hypertext mark-up language document and the software  
3 objects embedded in the document includes graphics image objects identified with universal  
4 resource locator data.

1 5. The automatically invoked intermediation process according to claim 1 further including  
2 the step of caching a copy of the downloaded purchased content at the transaction processing  
3 site for a time extending subsequent to the forwarding of the encrypted purchased content to  
4 the subscribing purchaser site.

1 6. The automatically invoked intermediation process according to claim 1 in which the access-  
2 restriction-override information corresponding to a restricted-access port in the subscriber-  
3 merchant accounts database includes a password for enabling access to content by way of the  
4 restricted-access port.

7. The automatically invoked intermediation process according to claim 1 in which the  
subscriber-purchaser accounts database includes for each subscribing purchaser information  
encoding an account-replenishment amount and a financial account number identifying an  
account at a financial institution upon which the subscribing purchaser may draw, the step (i)  
5 of debiting the purchaser account balance corresponding to the subscribing purchaser in the  
subscriber-purchaser accounts database by the access fee for accessing purchased content by  
way of the restricted-access port includes the step of comparing the purchaser account balance  
with an account minimum value and, if the purchaser account balance has fallen below the  
account minimum value, sending a funds-transfer request to the financial institution for  
10 transferring funds in the amount of the account-replenishment amount from the account  
identified by the financial account number to an intermediation entity account and, upon  
receipt at the transaction processing site of an approval of the transfer request, crediting the  
purchaser account balance by the account replenishment amount to bring the purchaser  
account balance above the account minimum value.

1 8. The automatically invoked intermediation process according to claim 7 in which the funds  
2 transfer request is sent from the transaction processing site to the financial institution over a  
3 communication channel separate from the digital communications network interconnecting the  
4 transaction processing site, the subscribing purchaser notes, and the subscribing merchant  
5 sites.

1 9. The automatically invoked intermediation process according to claim 1 in which the  
2 digital communications network interconnecting the transaction processing site, the  
3 subscribing purchaser sites, and the subscribing merchant sites is the Internet.

10. An automatically invoked intermediation process for purchasing content over a digital  
communications network by subscribing purchasers from subscribing merchants, the  
intermediation process comprising the steps of:

(a) establishing a database of subscriber-purchaser accounts and a  
5 database of subscriber-merchant accounts at a central transaction processing site on  
the digital communications network, the subscriber-merchant accounts database  
including information encoding resource locator data identifying at least one restricted-  
access port at each subscribing merchant site on the network and, for each such  
restricted-access port, information encoding an access fee schedule for accessing  
10 content by way of the restricted-access port and access-restriction-override  
information for enabling access to content by way of the restricted-access port, and the  
subscriber-purchaser accounts database including information encoding purchaser site  
authentication credentials and a purchaser account balance for each subscribing  
purchaser;

15 (b) at the network site of each subscribing purchaser, establishing a  
resource rules database including information encoding resource-locator-data  
identification criteria corresponding to each of at least a subset of the restricted-access  
ports at subscribing merchant sites identified in the subscriber-merchant accounts  
database and the access fee schedule for accessing content by way of the  
20 corresponding restricted-access port;

(c) at the network site of each subscribing purchaser, locally monitoring network communication activity information with respect to access to a target network resource generated by a browser program at the subscribing purchaser site and comparing such network communication activity information to the resource-locator-data identification criteria corresponding to restricted-access ports at the network sites of subscribing merchants in the resource rules database locally maintained at the site of the subscribing purchaser;

(d) in the event network communication activity information pertaining to the target network resource of step (c) matches with the resource-locator-data identification criteria corresponding to a restricted-access port in the resource rules database, retrieving the access fee schedule corresponding to the matched resource-locator-data identification criteria from the resource rules database, displaying an access fee from the access fee schedule for accessing content by way of the restricted access port corresponding to the resource-locator-data identification criteria, and prompting for approval or disapproval of completing the access for the displayed access fee;

(e) upon receipt at the subscribing purchaser site of a user communication responsive to the prompting of step (d) indicating approval of completing the access to content by way of the restricted-access port for the access fee, transmitting a purchase-request message from the subscribing purchaser site to the transaction processing site over the network, the purchase-request message including information encoding purchaser-site authentication credentials and identifying the restricted-access port at the merchant site corresponding to the matched resource-locator-data identification criteria;

(f) upon receipt of the purchase-request message of step (e) at the transaction processing site, determining whether the purchaser-site authentication credentials encoded in the purchase-request message matches with any purchaser-site authentication credentials included in the subscriber-purchaser accounts database and, if such a match is found, transmitting over the network to the restricted-access port of the merchant site a restricted-access-enabling access-request message to download

purchased content by way of the restricted-access port to the transaction processing site, the restricted-access-enabling access-request message including access-restriction-override information corresponding to the restricted-access port retrieved from the subscriber-merchant accounts database;

55

(g) upon receipt of the downloaded purchased content at the transaction processing site from the subscribing-merchant site by way of the restricted-access port responsive to the restricted-access-enabling access-request message of step (f), encrypting the downloaded purchased content and forwarding the thus encrypted purchased content to the subscribing purchaser site over the network;

60

(h) upon receipt of the encrypted purchased content of step (g) at the subscribing purchaser site, transmitting a content-received confirmation message to the transaction-processing site by the subscribing purchaser site over the network, the content received confirmation message including receipt-indicator the receipt-indicator data encoding whether or not a receipt data object with respect to purchased content had previously been received at the subscribing purchaser site;

65

(i) upon receipt of the content-received confirmation message of step (h) from the subscribing purchaser site at the transaction processing site, checking the receipt-indicator data to determine whether or not a receipt data object had previously been received with respect to the purchased content at the subscribing purchaser site, and, in the event no such receipt data object had been received, debiting the purchaser account balance corresponding to the subscribing purchaser in the subscriber-purchaser accounts database by the access fee for accessing purchased content by way of the restricted-access port, and forwarding a receipt-data object and a cryptographic key for decrypting the encrypted purchased content to the subscribing purchaser site over the network; and

70

75

(j) upon receipt of the cryptographic key at the subscribing purchaser site, decrypting the encrypted purchased content at the purchaser site.

11. The automatically invoked intermediation process according to claim 10 in which the receipt-indicator data included in the content received confirmation message of step (h) includes expiration date data encoding an expiration date for a receipt data object previously received at the subscribing purchaser site, and the step of checking the receipt indicator data of step (i) includes the step of comparing the expiration date data included in the receipt indicator data to a current date to determine if the expiration date encoded in the expiration date data has expired, and, in the event the expiration date has expired, debiting the purchaser account balance corresponding to the subscribing purchaser in the subscriber purchaser accounts database by the access fee for accessing purchased content by way of the restricted-access port.

12. The automatically invoked intermediation process according to claim 11 in which the receipt-indicator data included in the content received confirmation message of step (h) includes receipt verification check data for testing whether a receipt data object previously received at the subscribing purchaser site is genuine, and the step of checking the receipt indicator data of step (i) includes the step of testing the verification check data to determine if the receipt data object is genuine, and, in the event the receipt data object is not genuine, debiting the purchaser account balance corresponding to the subscribing purchaser in the subscribing purchaser accounts database by the access fee for accessing purchased content by way of the restricted-access port.

13. An automatically invoked intermediation process for purchasing hard goods over a digital communications network by subscribing purchasers from subscribing merchants, the intermediation process comprising the steps of:

(a) establishing a database of subscriber-purchaser accounts and a database of subscriber-merchant accounts at a central transaction processing site on the digital communications network, the subscriber-merchant accounts database including information encoding resource locator data identifying at least one order-entry port at each subscribing merchant site on the network and, for each such order-entry port, information encoding a schedule of prices and goods purchasable by orders entered by way of the order-entry port, and the subscriber-purchaser accounts database

including information encoding purchaser site authentication credentials and a purchaser account balance for each subscribing purchaser;

15 (b) at the network site of each subscribing purchaser, establishing a resource rules database including information encoding resource-locator-data identification criteria corresponding to each of at least a subset of the order-entry ports at subscribing merchant sites identified in the subscriber-merchant accounts database and the schedule of prices and goods purchasable by orders entered by way of the corresponding order-entry port;

20 (c) at the network site of each subscribing purchaser, locally monitoring network communication activity information with respect to access to a target network resource generated by a browser program at the subscribing purchaser site and comparing such network communication activity information to the resource-locator-data identification criteria corresponding to order-entry ports at the network sites of  
25 subscribing merchants in the resource rules database locally maintained at the site of the subscribing purchaser;

(d) in the event network communication activity information pertaining to the target network resource of step (c) matches with the resource-locator-data identification criteria corresponding to a order-entry port in the resource rules  
30 database, retrieving the schedule of prices and goods corresponding to the matched resource-locator-data identification criteria from the resource rules database, displaying at least a portion of prices and goods from the schedule, and prompting for identification of goods to be ordered;

(e) upon receipt at the subscribing purchaser site of a user  
35 communication responsive to the prompting of step (d) identifying hard goods to be ordered, transmitting an order-request message from the subscribing purchaser site to the transaction processing site over the network, the order-request message including information encoding purchaser-site authentication credentials, identifying the order-entry port at the merchant site corresponding to the matched resource-locator-data  
40 identification criteria, and specifying the hard goods to be ordered;

45 (f) upon receipt of the order-request message of step (e) at the transaction processing site, determining whether the purchaser-site authentication credentials encoded in the order-request message matches with any purchaser-site authentication credentials included in the subscriber-purchaser accounts database and, if such a match is found, transmitting over the network to the order-entry port of the merchant site an order-entry message to enter an order for the hard goods specified in the order-request message by way of the order-entry port and request transmission of an order-confirmation message from the merchant site to the transaction processing site;

50 (g) upon receipt of an order-confirmation message at the transaction processing site from the subscribing merchant site responsive to the order-entry message of step (f), encrypting the order-confirmation message and forwarding the encrypted order confirmation message to the subscribing purchaser site over the digital communications network;

55 (h) upon receipt of the encrypted order-confirmation message of step (g) at the subscribing purchaser site, transmitting an order-confirmation received message to the transaction-processing site by the subscribing purchaser site over the network;

60 (i) upon receipt of the order-confirmation message of step (h) from the subscribing purchaser site at the transaction processing site, debiting the purchaser account balance corresponding to the subscribing purchaser in the subscriber-purchaser accounts database by the total price of the hard goods ordered and forwarding a cryptographic key for decrypting the encrypted order-confirmation message to the subscribing purchaser site over the network; and

65 (j) upon receipt of the cryptographic key at the subscribing purchaser site, decrypting the encrypted order-confirmation message at the purchaser site.

14. The automatically invoked intermediation process according to claim 13 in which the subscriber-purchaser accounts database includes for each subscribing purchaser information encoding an account-replenishment amount and a financial account number identifying an



account at a financial institution upon which the subscribing purchaser may draw, the step (i) of debiting the purchaser account balance corresponding to the subscribing purchaser in the subscriber-purchaser accounts database by the total price of the hard goods ordered includes the step of comparing the purchaser account balance with an account minimum value and, if the purchaser account balance has fallen below the account minimum value, sending a funds-transfer request to the financial institution for transferring funds in the amount of the account-replenishment amount from the account identified by the financial account number to an intermediation entity account and, upon receipt at the transaction processing site of an approval of the transfer request, crediting the purchaser account balance by the account replenishment amount to bring the purchaser account balance above the account minimum value.

15. The automatically invoked intermediation process according to claim 14 in which the funds transfer request is sent from the transaction processing site to the financial institution over a communication channel separate from the digital communications network interconnecting the transaction processing site, the subscribing purchaser notes, and the subscribing merchant sites.

16. The automatically invoked intermediation process according to claim 13 in which the digital communications network interconnecting the transaction processing site, the subscribing purchaser sites, and the subscribing merchant sites is the Internet.

1/23

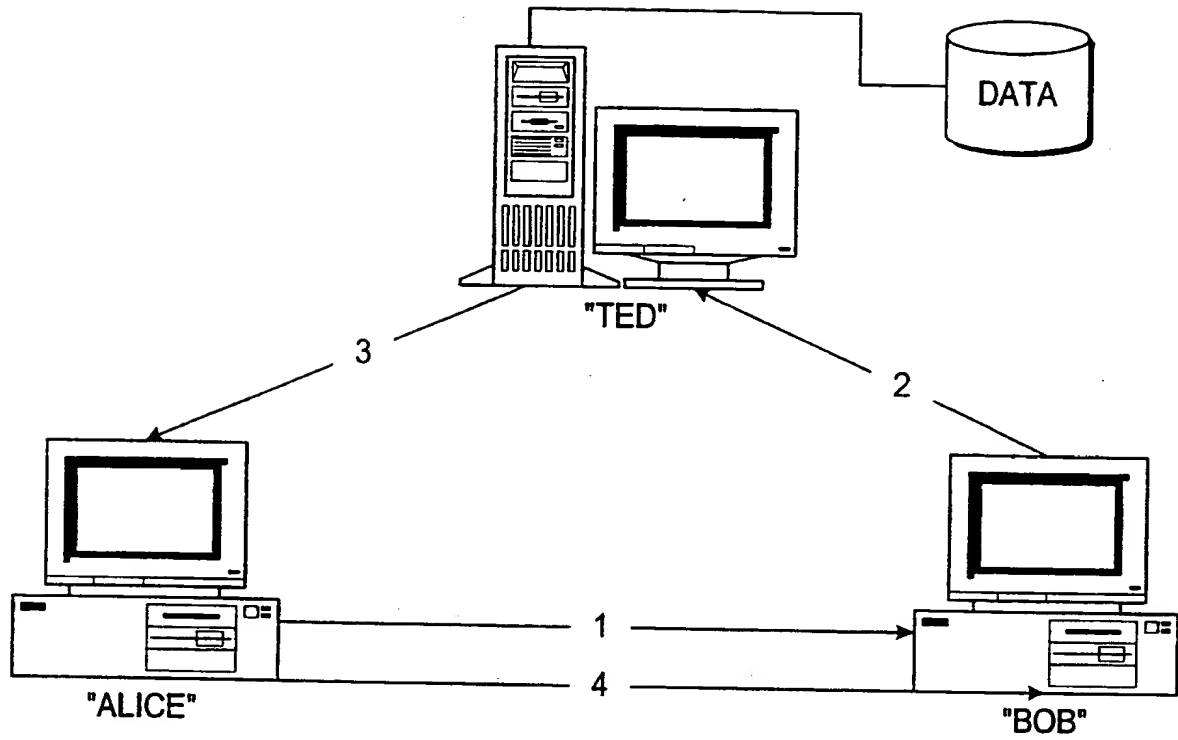
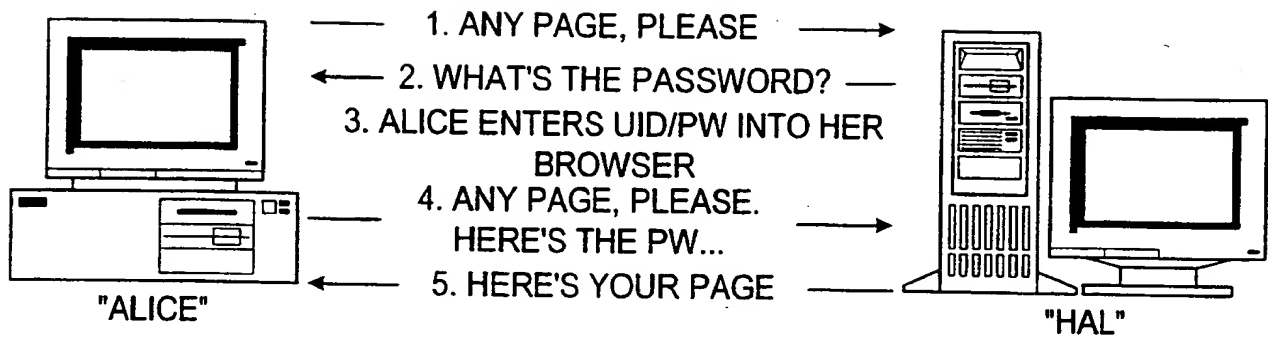


FIG. 1

2/23



**FIG. 2**  
PRIOR ART

3/23

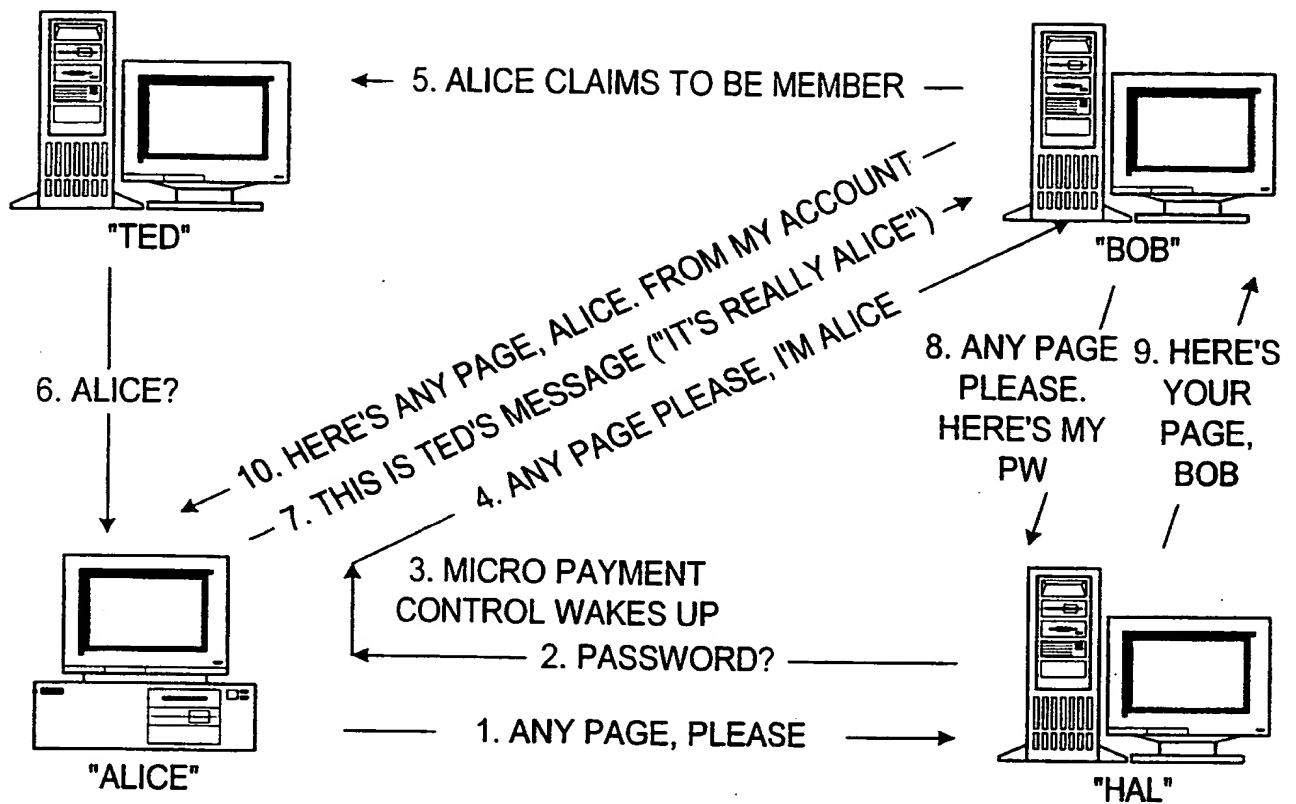


FIG. 3

4/23

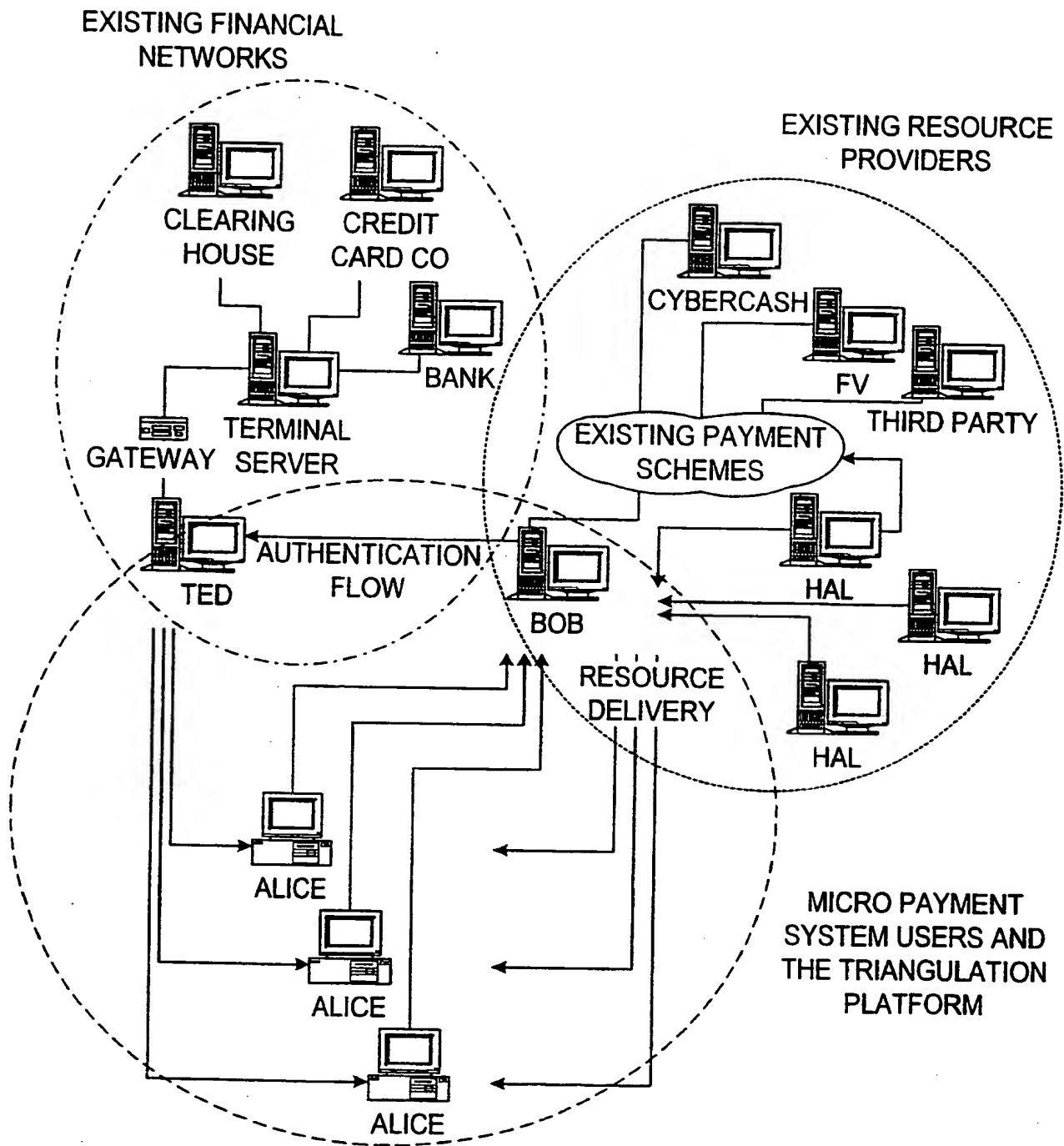


FIG. 4

5/23

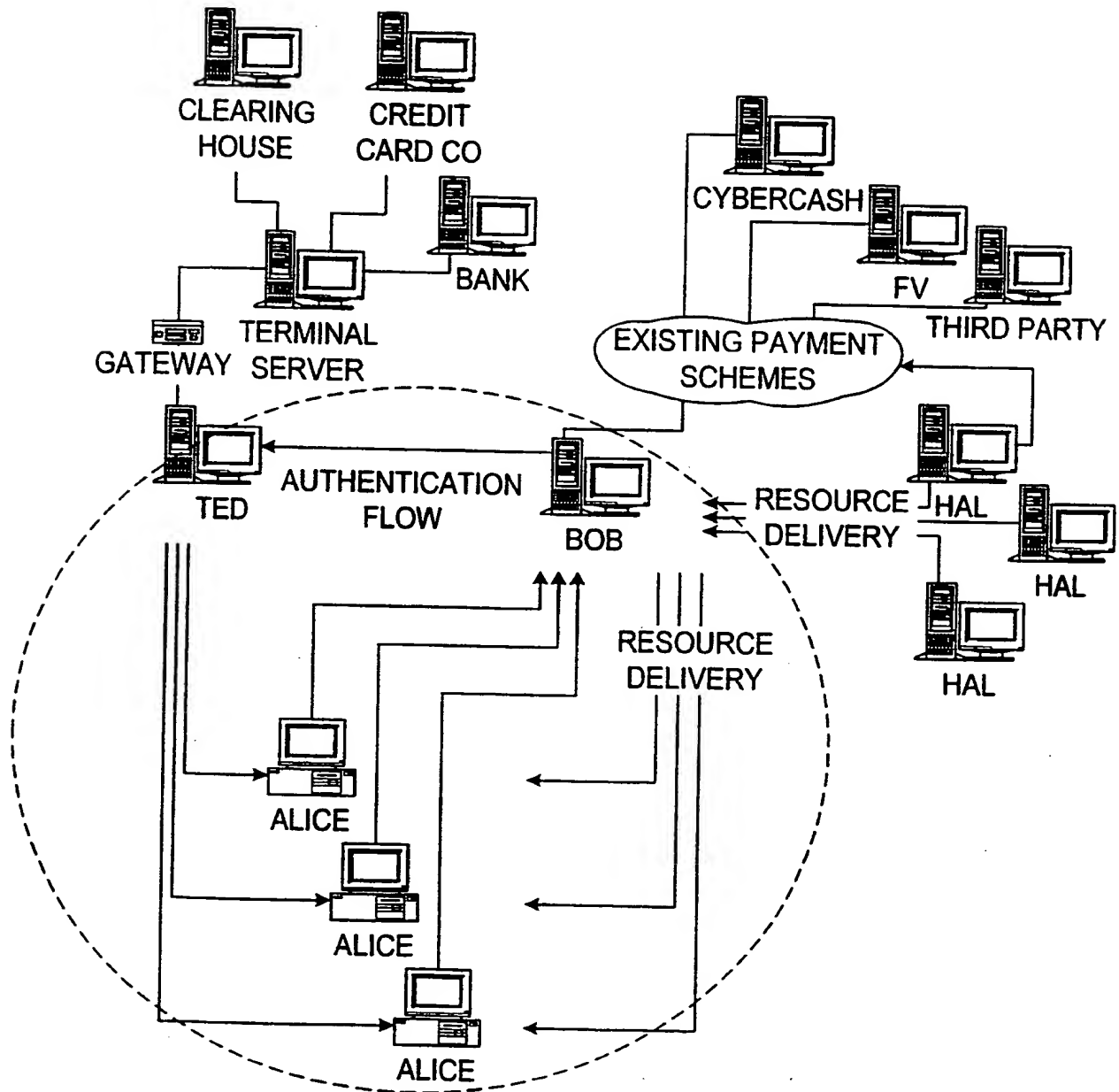


FIG. 5

6/23

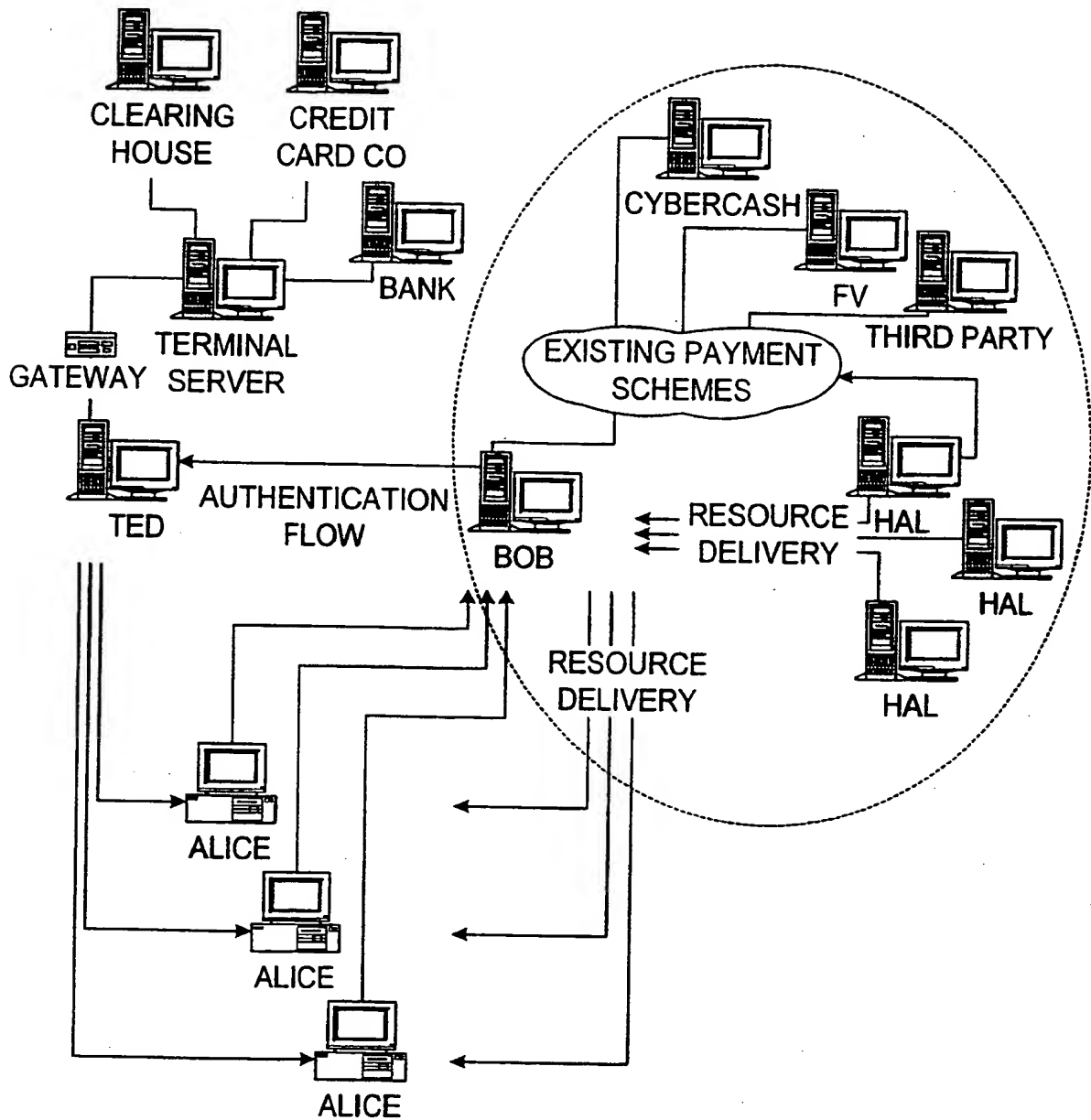


FIG. 6

7/23

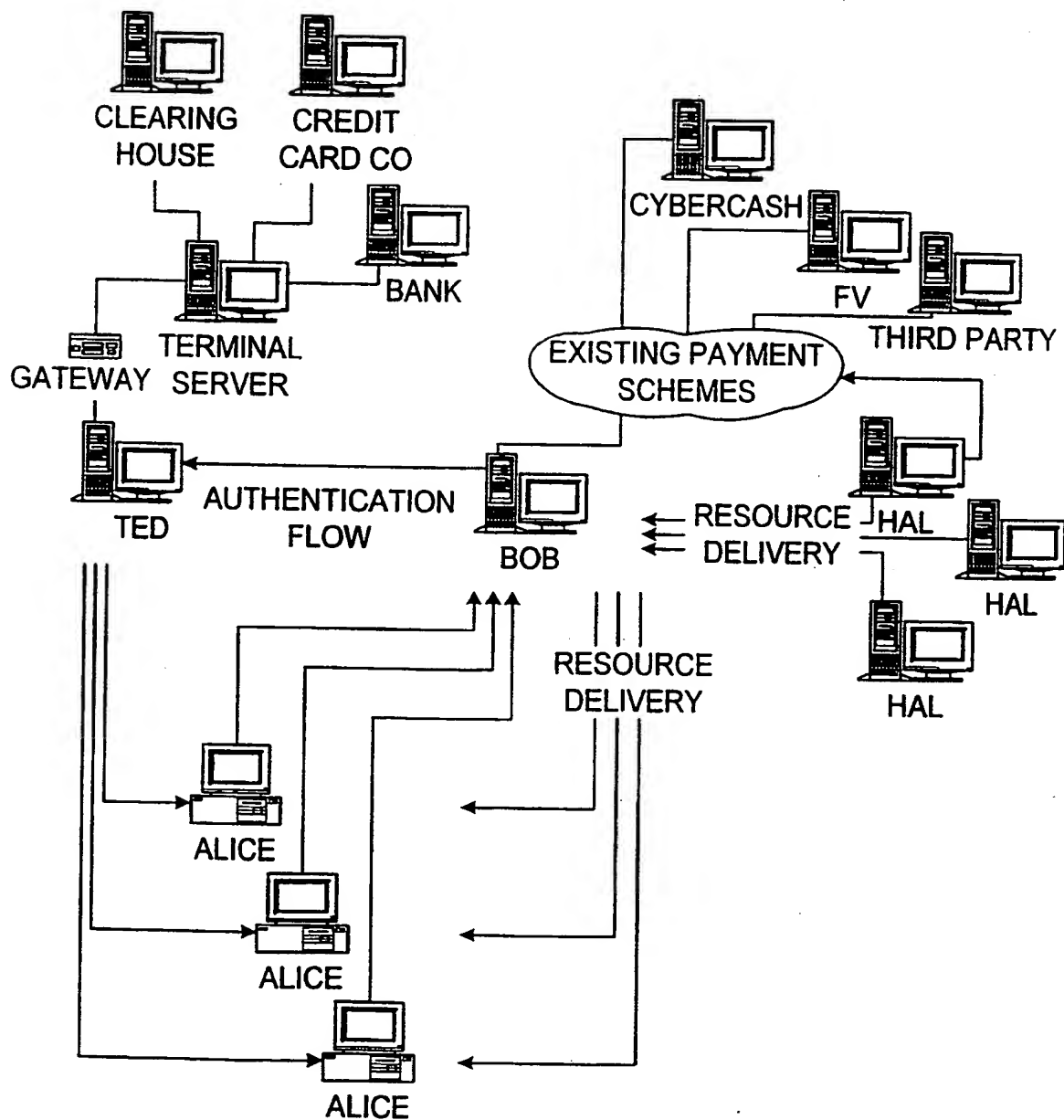


FIG. 7



8/23

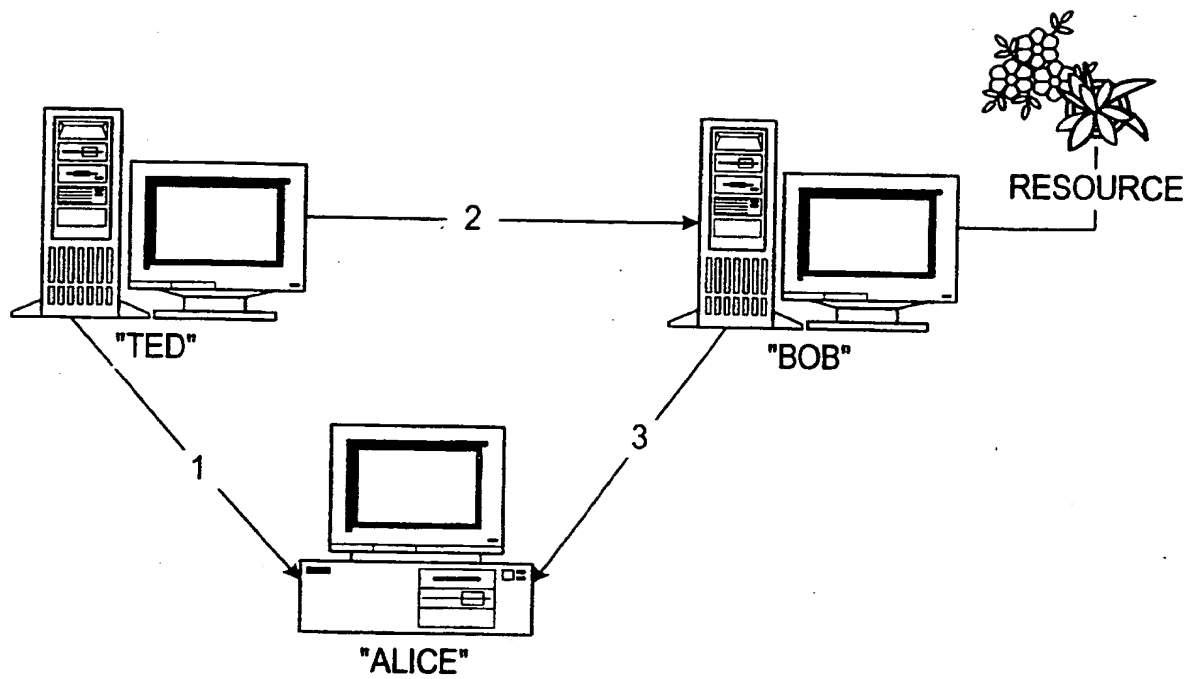


FIG. 8

9/23

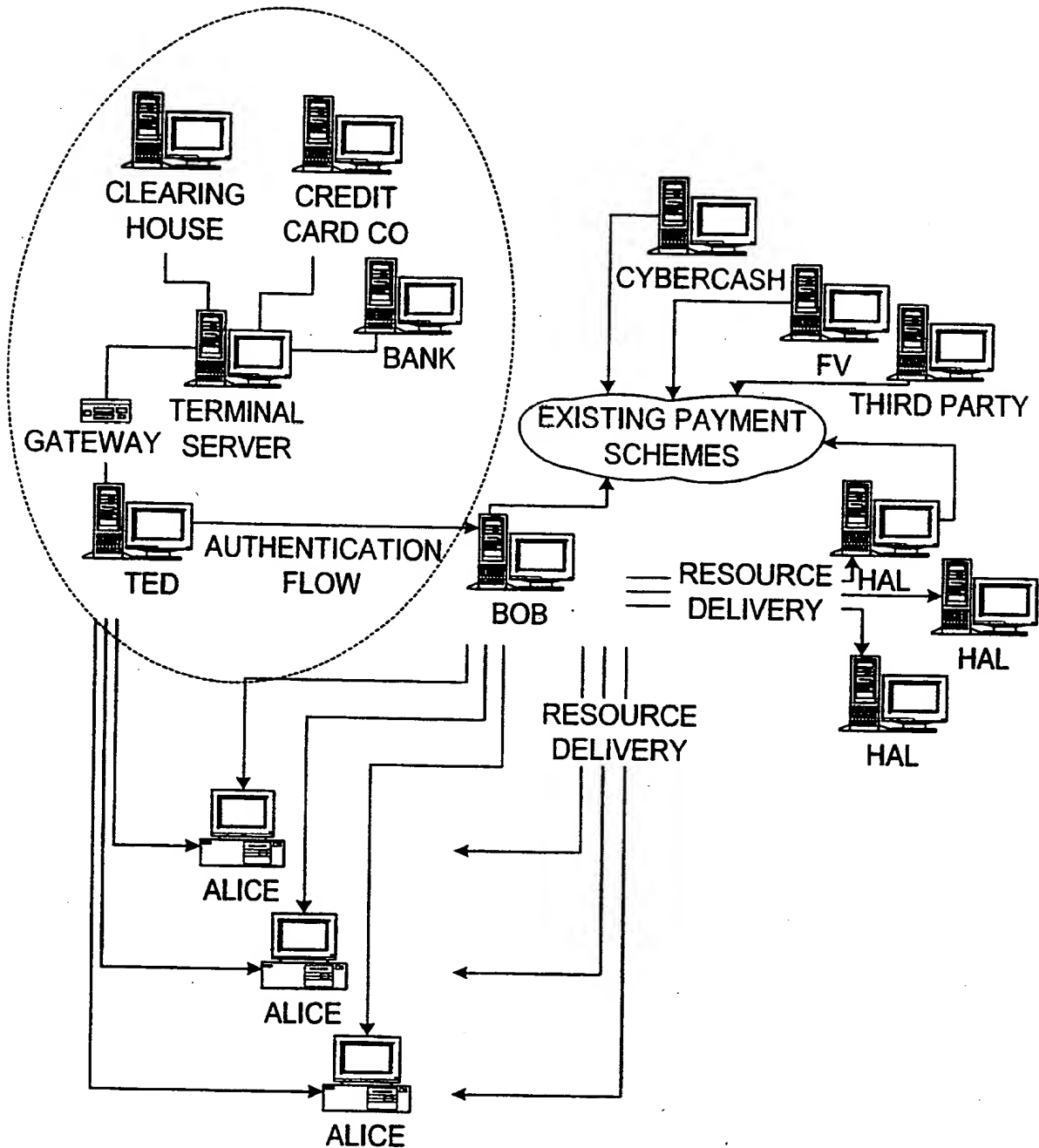


FIG. 9

10/23

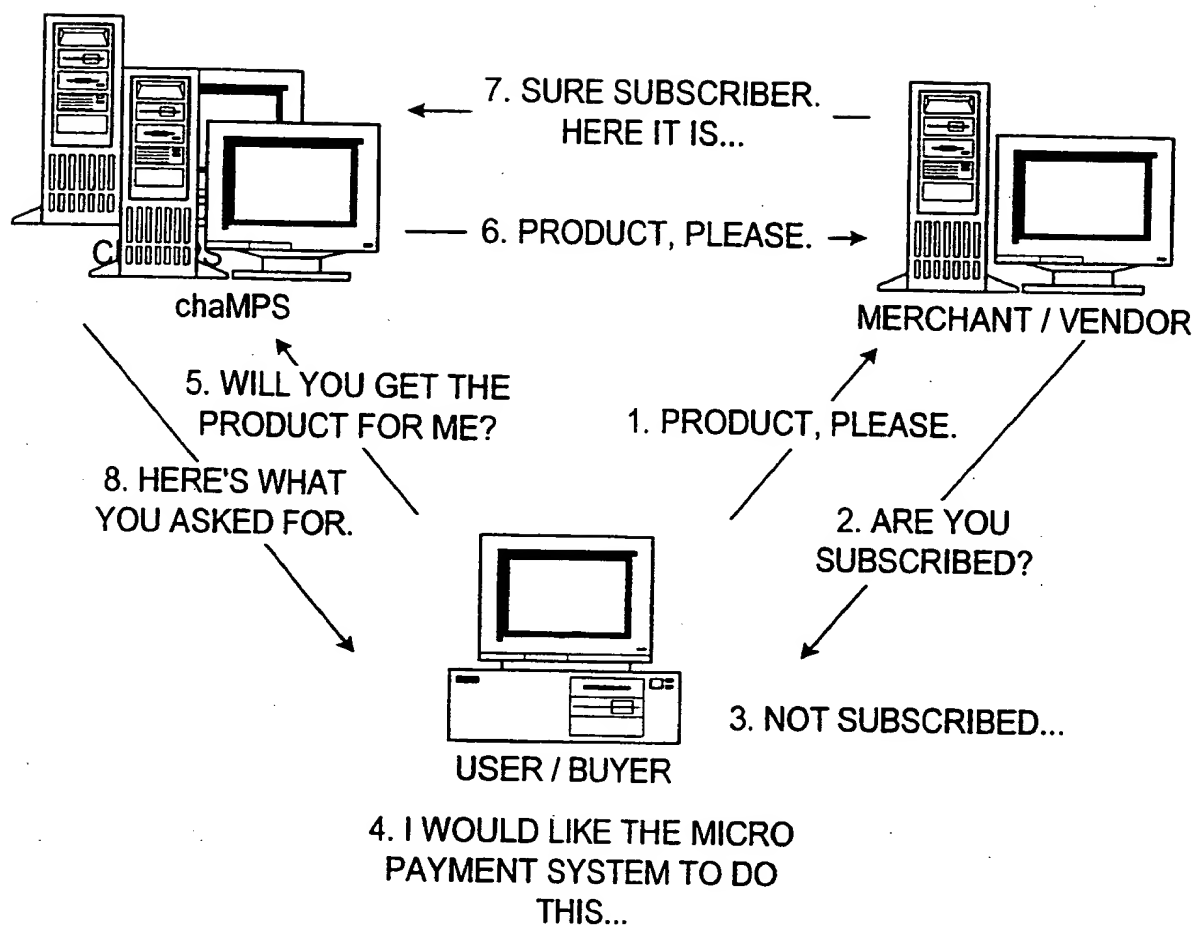


FIG. 10

11/23

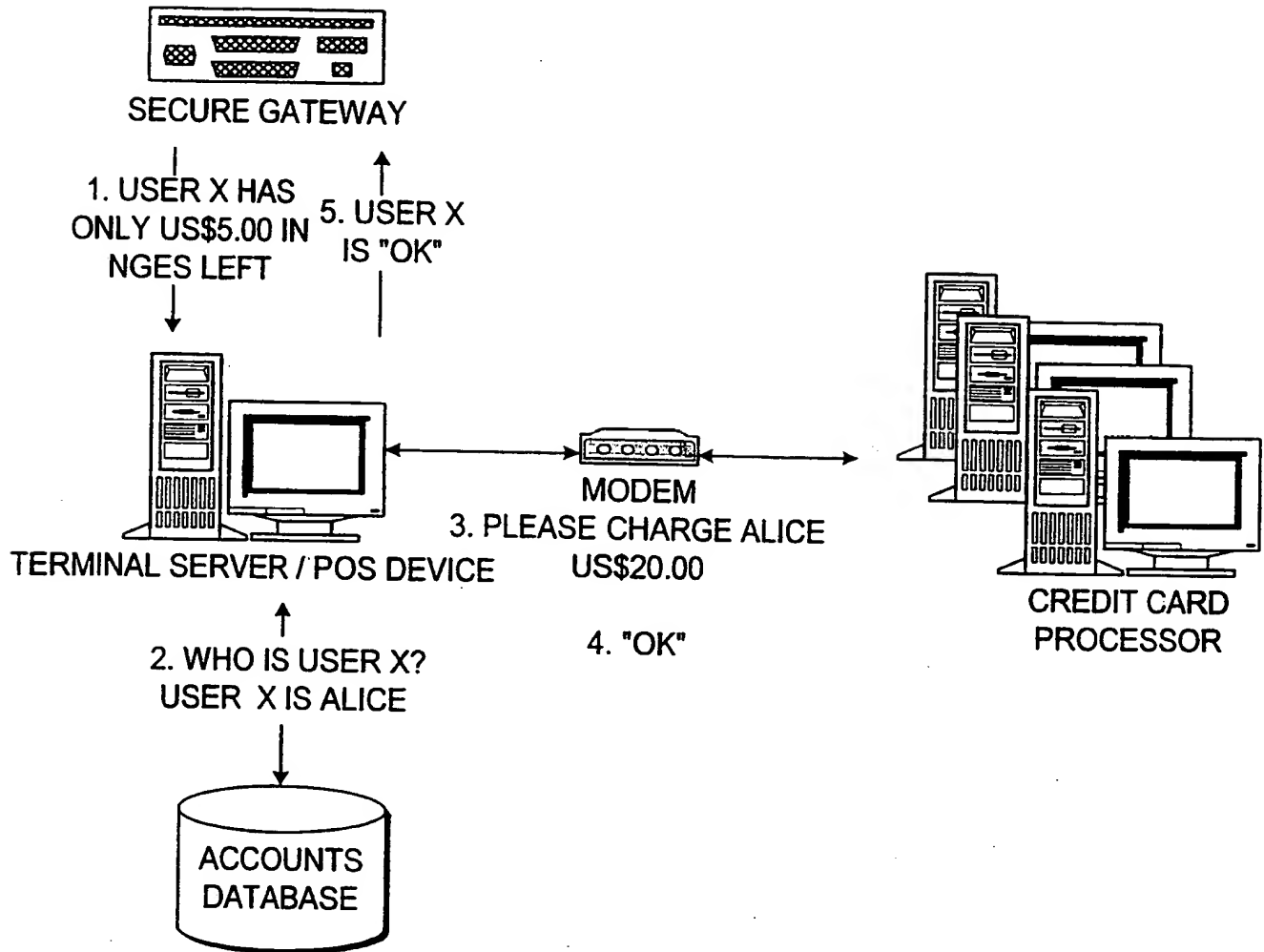


FIG. 11

12/23

FIG. 12A

## MERCHANT ACCOUNT PRE-APPLICATION

TO GET STARTED, FILL OUT THIS PRE-APPLICATION AND FAX IT OR SEND IT TO POINT OF SALE SYSTEMS. ALONG WITH A CHECK FOR \$75, WHICH WILL BE CREDITED TOWARDS THE APPLICATION FEE. IF YOU ARE GOING WITH OUR \$20 DOWN PROGRAM, YOU WOULD SIMPLY SEND US THE \$20. **THIS FEE IS REFUNDED TO YOU IF YOU ARE DECLINED FOR ANY REASON EXCEPT FOR DEROGATORY CREDIT OR LACK OF CREDIT.** IF YOU FAX A CHECK, WE WILL REPRODUCE IT AND DEPOSIT IT AT OUR BANK, PNC BANK IN BENSALEM, PA. YOU WILL RECEIVE IT BACK AS A CANCELED CHECK WITH YOUR OTHER CHECKS. WE REQUEST THIS FEE IN ADVANCE BECAUSE WE DO NOT SIMPLY SEND OUT APPLICATIONS TO PEOPLE WHO ARE STILL SEARCHING FOR A BETTER DEAL OR COMPARING OFFERS OR WHO ARE NOT READY TO GET SET UP YET. APPLICATIONS AND POSTAGE COST US ABOUT \$3 EACH. SINCE ONLY 1 OUT OF 10 PEOPLE SEND APPLICATIONS BACK, IT COSTS US ABOUT \$30 IN WASTED EXPENSE FOR EACH MERCHANT WHO APPLIES. IF YOU SIMPLY WANT AN APPLICATION AND ARE NOT COMMITTED TO SIGNING UP, SEND US \$30 AND WE WILL SEND YOU A BLANK APPLICATION. IF YOU WANT YOUR \$30 BACK, RETURN THE BLANK APPLICATION TO US. WHEN WE RECEIVE THIS APPLICATION, WE WILL FILL OUT A HARD COPY VERSION AND RETURN IT TO YOU FOR YOUR SIGNATURE. WHEN YOU SEND IT BACK IN, YOU WOULD THEN SEND IN THE REQUIRED SUPPORTING MATERIAL, SUCH AS COPIES OF ANY ADS, BROCHURES OR FLIERS, OR A PRINT OUT OF YOUR EXISTING OR PROPOSED WEB SITE, ALONG WITH A PHOTO OF THE OUTSIDE OF YOUR HOME OR BUSINESS, SHOWING THE PHYSICAL ADDRESS. AN INSIDE PHOTO SHOWING YOUR PRODUCT, INVENTORY OR OFFICE SET UP IS ALSO REQUIRED. DEPENDING ON THE PROGRAM YOU HAVE SELECTED, A COPY OF A BUSINESS LICENSE OR BUSINESS NAME REGISTRATION MAY BE REQUIRED.

## BUSINESS INFORMATION

LEGAL NAME OF BUSINESS:	BUSINESS START DATE: _____ # LOCATIONS: _____
DBA NAME:	MONTHLY VOLUME: _____ AVERAGE TICKET: _____
PHYSICAL ADDRESS:	TYPE OF BUSINESS: RETAIL, MAIL ORDER, SERVICE
CITY, STATE, ZIP:	PRODUCT OR SERVICE SOLD:
CONTACT NAME:	CARD PRESENT: _____ % CARD NOT PRESENT: _____ %
PHONE NUMBER:	FAX NUMBER: _____

## OWNER INFORMATION

<input type="checkbox"/> SOLE PROP	<input type="checkbox"/> PARTNERSHIP	<input type="checkbox"/> CORP	<input type="checkbox"/> OTHER: _____	TAX ID#(CAN USE SSN):
OWNER 1/PARTNER/OFFICER NAME:		TITLE IN BUSINESS:		SOCIAL SECURITY #:
HOME ADDRESS:		CITY/ST/ZIP:		PHONE NUMBER:
OWNER 2/PARTNER/OFFICER NAME:		TITLE IN BUSINESS:		SOCIAL SECURITY #:
HOME ADDRESS:		CITY/ST/ZIP:		PHONE NUMBER:

SUBSTITUTE SHEET (RULE 26)

13/23

FIG. 12B

## BANK &amp; TRADE REFERENCE INFORMATION

BANK NAME:	CONTACT:	PHONE NUMBER:	ACCOUNT #:
TRADE REFERENCE:	CONTACT:	PHONE NUMBER:	ACCOUNT #:
TRADE REFERENCE:	CONTACT:	PHONE NUMBER:	ACCOUNT #:
TRADE REFERENCE:	CONTACT:	PHONE NUMBER:	ACCOUNT #:

## FEE SCHEDULE INFORMATION

SELECT THE APPROPRIATE PROGRAM BASED ON THE RATES &amp; FEES SECTION OF OUR INFORMATION.

## PROGRAM 1 (PROCESS BY TELEPHONE)

DISCOUNT RATE: 2.49%	TRANSACTION CHARGE: 50 CENTS	MONTHLY MIN. FEE: \$20	STATEMENT FEE: \$20
----------------------	------------------------------	------------------------	---------------------

SET UP FEE: \$295, INCLUDES THE \$75 APPLICATION FEE PAID WITH THIS PRE-APPLICATION. UPON APPROVAL, YOU WILL RECEIVE INSTRUCTIONS ON HOW TO USE THE PHONE PROCESS METHOD. NO EQUIPMENT IS NEEDED. ADDRESS VERIFICATION IS SUPPORTED ON THIS SYSTEM. THIS PROGRAM IS FOR TANGIBLE PRODUCTS ONLY, NOT SERVICES. THIS SERVICE IS PROVIDED BY MCCS, AN AGENT FOR WOODFOREST BANK, HOUSTON TX. MEMBER FDIC

## PROGRAM 2 (NO MONTHLY STATEMENT FEE, \$20 MONTHLY MINIMUM FEE)

CARD SWIPED DISCOUNT RATE (NON-COMPUTERS): 1.49%	TRANSACTION CHARGE: 20 CENTS
CARD SWIPED DISCOUNT RATE (COMPUTERS): 1.69%	TRANSACTION CHARGE: 20 CENTS

A 1% KEYED-IN SURCHARGE APPLIES TO THE ABOVE DISCOUNT RATES.

MAIL/PHONE ORDER DISCOUNT RATE (NON-COMPUTERS): 2.29%	TRANSACTION CHARGE: 30 CENTS
MAIL/PHONE ORDER DISCOUNT RATE (COMPUTERS): 2.69%	TRANSACTION CHARGE: 30 CENTS

THIS PROGRAM REQUIRES GOOD PERSONAL CREDIT (NO EXCESSIVE CHARGEOFFS OF COLLECTION ACCOUNTS). CREDIT PROBLEMS DUE TO MEDICAL BILLS OR OTHER UNEXPECTED EMERGENCIES ARE OVERLOOKED. DEPENDING ON CREDIT AND TYPE OF BUSINESS, PROCESSING BANK MAY REQUIRE COPIES OF LAST YEAR'S TAX RETURN AND THREE MONTH'S MOST RECENT CHECKING ACCOUNT STATEMENTS, TO VERIFY THAT YOU HAVE AN INCOME OUTSIDE OF CREDIT CARD SALES.

## PROGRAM 3 (NO MONTHLY MINIMUM FEE, \$10 MONTHLY STATEMENT FEE)

CARD SWIPED DISCOUNT RATE (NON-COMPUTERS): 1.49%	TRANSACTION CHARGE: 20 CENTS
CARD SWIPED DISCOUNT RATE (COMPUTERS): 1.69%	TRANSACTION CHARGE: 20 CENTS

A 1% KEYED-IN SURCHARGE APPLIES TO THE ABOVE DISCOUNT RATES. A 7 DAY RESERVE ACCOUNT MAY BE NEEDED ON NEW OR MAIL ORDER BUSINESSES. A \$50 SITE INSPECTION FEE IS ALSO REQUIRED. PROPERTY RESOURCE NETWORK WILL CALL YOU TO SET UP AN APPOINTMENT TO VISIT YOU TO VERIFY YOUR BUSINESS AND TAKE THE NEEDED PHOTOS.

MAIL/PHONE ORDER DISCOUNT RATE (NON-COMPUTERS): 1.99%	TRANSACTION CHARGE: 30 CENTS
MAIL/PHONE ORDER DISCOUNT RATE (COMPUTERS): 2.69%	TRANSACTION CHARGE: 30 CENTS

THIS PROGRAM REQUIRES A COPY OF A BUSINESS LICENSE, A FICTITIOUS NAME REGISTRATION OR A COPY OF YOUR CERTIFICATE OF INCORPORATION. A BUSINESS CHECKING ACCOUNT IS ALSO NEEDED. A COPY OF A DRIVER'S LICENSE IS ALSO NEEDED

14/23

PROGRAM 4 (FOR MERCHANTS WITH LIMITED OR BAD PERSONAL CREDIT - \$95 APP FEE)		
CARD SWIPED DISCOUNT RATE (NON-COMPUTERS): 1.69%	TRANSACTION CHARGE: 20 CENTS	
CARD SWIPED DISCOUNT RATE (COMPUTERS): 1.89%	TRANSACTION CHARGE: 20 CENTS	
A 1% KEYED-IN SURCHARGE APPLIES TO THE ABOVE DISCOUNT RATES. THERE IS A \$25 MONTHLY MINIMUM FEE AND A \$10 MONTHLY STATEMENT FEE. THE APPLICATION FEE IS \$95.		
MAIL/PHONE ORDER DISCOUNT RATE (NON-COMPUTER): 2.69%	TRANSACTION CHARGE: 30 CENTS	
MAIL/PHONE ORDER DISCOUNT RATE (COMPUTERS): 2.99%	TRANSACTION CHARGE: 30 CENTS	

BASED ON MY BUSINESS TYPE AND NEEDS, I HAVE SELECTED PROGRAM \_\_\_\_.  
 MY TYPE OF BUSINESS IS \_\_CARD SWIPED, \_\_NON-CARD SWIPED(SELECT ONE).

EQUIPMENT SELECTION			
EQUIPMENT TYPE	PURCHASE PRICE	24 MONTH LEASE	SUPPORTS AVS ?
VERIFONE ZON XL	\$395	\$27/MONTH	NO
VERIFONE PRINTER	\$295	\$18/MONTH	N/A
VERIFONE TRANZ 330	\$495	\$29/MONTH	PROGRAMS 3 & 4
VERIFONE TRANZ 380	\$595	\$34/MONTH	PROGRAMS 2,3 & 4
VERIFONE TRANZ 460	\$695	\$39/MONTH	PROGRAMS 3 & 4
VERIFONE TRANZ 420	\$795	\$44/MONTH	PROGRAMS 3 & 4
HYPERCOM T7P	\$695	\$39/MONTH	PROGRAMS 2,3 & 4
POS CHARGE	\$395	\$27/MONTH	PROGRAMS 2,3 & 4
MAC AUTHORIZE	\$495	\$29/MONTH	PROGRAMS 2,3 & 4

AN OPTIONAL 24 MONTH LEASE IS AVAILABLE INSTEAD OF PURCHASING THE EQUIPMENT. THE LEASING COMPANY ALSO CHARGES YOUR STATE SALES TAX RATE PLUS A \$2.50 PER MONTH LOSS AND DESTRUCTION WAIVER. LEASE APPROVAL IS BASED ON YOUR PERSONAL CREDIT.

I HAVE SELECTED THE FOLLOWING EQUIPMENT: \_\_\_\_\_. I WISH TO \_\_PURCHASE. \_\_LEASE IT (SELECT ONE).

I ALREADY HAVE THE FOLLOWING EQUIPMENT: \_\_\_\_\_. I WISH TO HAVE IT REPROGRAMMED FOR FEE OF \$150, IN ADDITION TO THE APPLICATION FEE.

FAX OR MAIL THIS PRE-APPLICATION TODAY!

I WISH TO APPLY FOR A MERCHANT ACCOUNT BASED ON THE ABOVE INFORMATION. I AM ENCLOSING A CHECK MADE PAYABLE TO POINT OF SALE SYSTEMS FOR \$75, WHICH IS REFUNDED IF MY ACCOUNT IS DECLINED FOR ANY REASON EXCEPT FOR DEROGATORY OR LACK OF CREDIT.

SIGNED: \_\_\_\_\_

DATE: \_\_\_\_\_

FAX THIS PAPERWORK AND A CHECK TO 215-245-5770. POINT OF SALE SYSTEMS MAINTAINS A CHECKING ACCOUNT AT PNC BANK, BENSALEM, PA. YOUR CHECK WILL BE PRINTED ON OUR CHECK PRINTING SYSTEM AND DEPOSITED. YOU WILL GET IT BACK AS A CANCELED CHECK. YOU CAN ALSO MAIL THIS PACKAGE TO:

POINT OF SALE SYSTEMS  
 1234 BAYBERRY RD  
 BENSALEM, PA 19020

I WISH TO HAVE MY WEB PAGE REGISTERED WITH OVER 200 SEARCH ENGINES AND DIRECTORIES AT NO COST. I HAVE PROVIDED THE FOLLOWING INFORMATION:

WEB PAGE URL: \_\_\_\_\_

EMAIL ADDRESS: \_\_\_\_\_

FIG. 12C

15/23

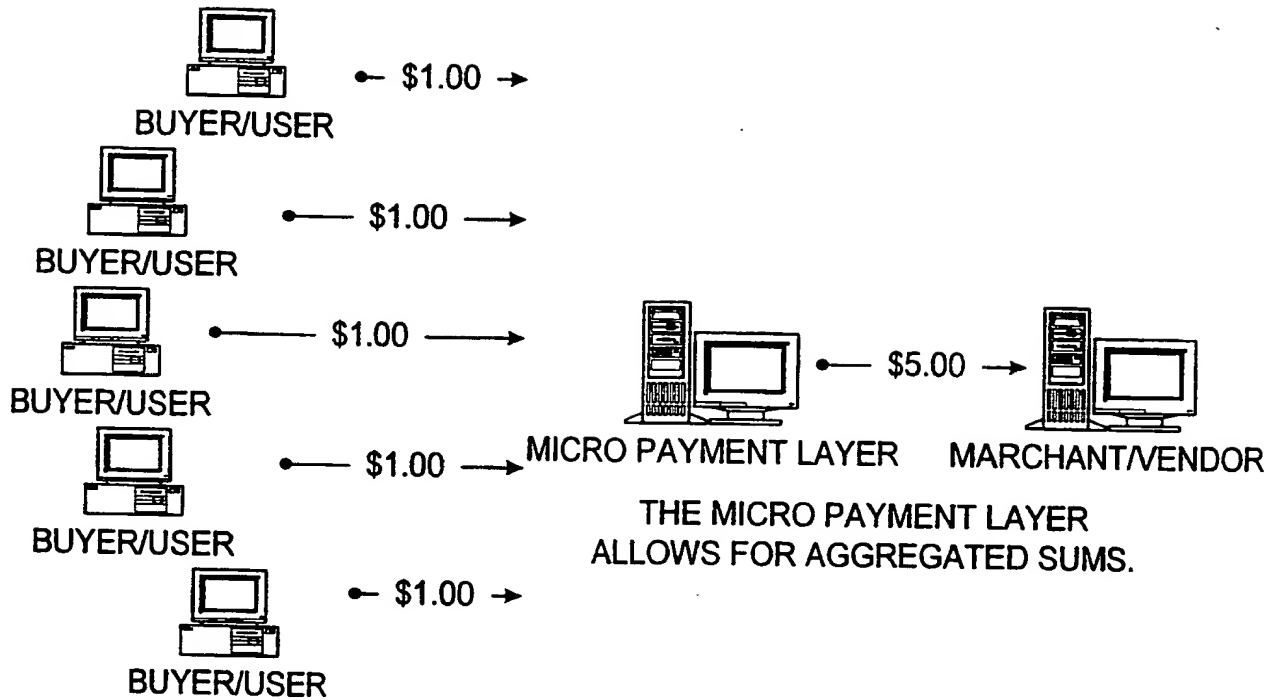
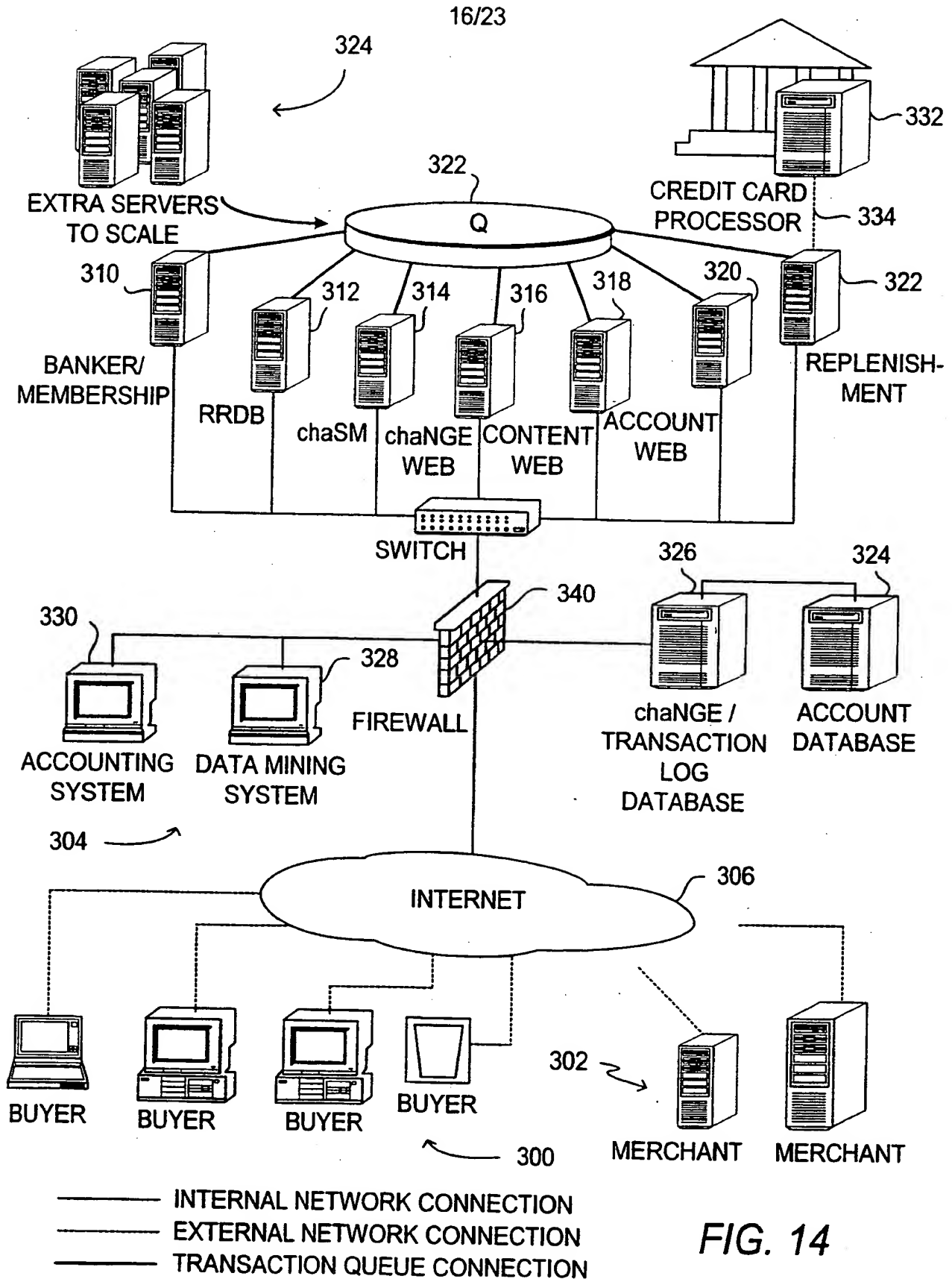


FIG. 13





17/23

402 →	CONTACT INFORMATION			
	LAST NAME	<input type="text"/>		
	FIRST NAME	<input type="text"/>	MIDDLE INITIAL	<input type="text"/>
	ADDRESS	<input type="text"/>		
		<input type="text"/>		
404 →	CITY	<input type="text"/>	STATE/PROVINCE	<input type="text"/>
	COUNTRY	<input type="text"/>	ZIP CODE	<input type="text"/> - <input type="text"/>
	EMAIL	<input type="text"/>		
	BILLING INFORMATION			
406 →	CREDIT CARD #	<input type="text"/>		
	CARD TYPE	<input type="text"/> PLEASE SELECT <input checked="" type="checkbox"/>	EXPIRATION	<input type="text"/>
	REPLENISHMENT INFORMATION			
408 →	INITIAL DEPOSIT	\$20 <input type="text"/> .00	REPLENISHMENT TYPE	<input checked="" type="checkbox"/> AUTOMATIC <input type="checkbox"/>
400 →	REPLENISHMENT THRESHOLD	\$10 <input type="text"/> .00	REPLENISHMENT AMOUNT	\$20 <input type="text"/> .00

FIG. 15

18/23

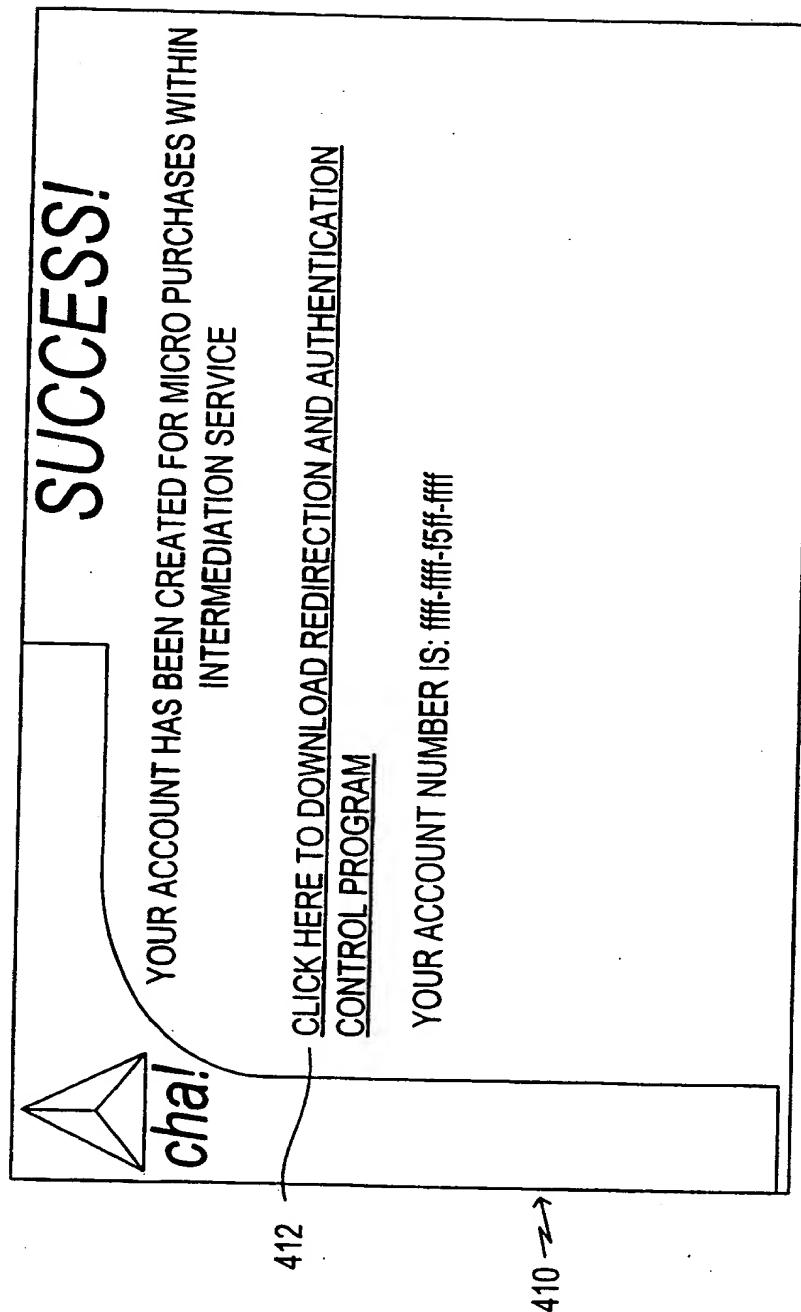


FIG. 16

19/23

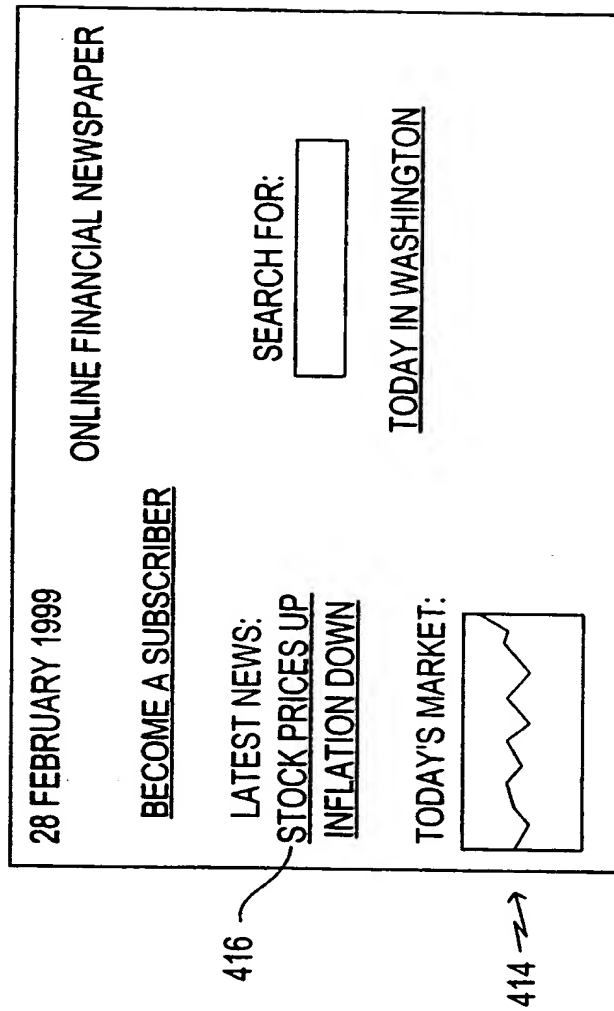


FIG. 17

20/23

THE PAGE YOU REQUESTED IS AVAILABLE ONLY TO SUBSCRIBERS.

<p><b>IF YOU SUBSCRIBE</b></p> <p>USER NAME: <input style="width: 100%;" type="text"/></p> <p>PASSWORD: <input style="width: 100%;" type="password"/></p> <p style="text-align: center;"><input type="button" value="SIGN ON"/></p> <p><input type="checkbox"/> SAVE MY USER NAME AND PASSWORD  <a href="#">MORE INFORMATION ABOUT THIS FEATURE</a></p>	<p><b>IF YOU DO NOT SUBSCRIBE</b></p> <ul style="list-style-type: none"> <li>• <a href="#">LEARN ABOUT SUBSCRIBING TO THE ONLINE FINANCIAL NEWSPAPER</a></li> <li>• <a href="#">REGISTER NOW AS A NEW SUBSCRIBER</a></li> </ul> <div style="border: 1px solid black; height: 20px; width: 100%; margin-top: 10px;"></div>
---	---

FIG. 18

420 →

→ 418

8708	11
8701	1
8695	3

SEARCH

RECORD FIRMS FORM COALITION TO COMBAT AMERICANS SHRUG OFF INVASION BY FOREIGN CREDIT-CARD ISSUERS ARE HOPING TO HAVE

RECENT SPECIAL REPORTS

SELLING POINTS, E-COMMERCE, CONTENT A BREAKAWAY; FOCUS ON SMALL BUSINESS PERSONAL FINANCE

FOR

GO DIRECTLY TO: FRONT PAGE GO

ECONOMY

FINANCIAL MARKETS

GOVERNMENT & POLITICS

INDUSTRIES

LAW

REFERENCE

SMALL BUSINESS

OTHER CATEGORIES

428

426

HEY, DO YOU WANT TO USE chaMPS?

DESCRIPTION: O.F.N.

PRICE: \$0.50

DURATION: 2 HOURS

OK

CANCEL

INVITED TO EONE ON

422

FIG. 19

414

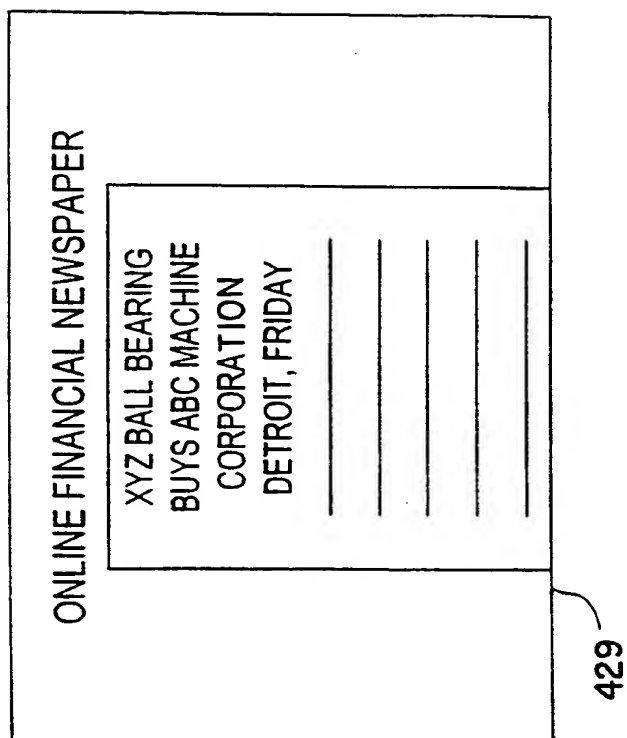



FIG. 20

23/23



# ACCOUNT MAINTENANCE

DEPOSIT

WITHDRAWAL

ACCOUNT INFO

TRANSACTION HISTORY

LAST 10 TRANSACTIONS

GO

MEMBER: PANNL MORSHEDI ACCOUNT BALANCE:

\$19.50

DATE	DESCRIPTION	AMOUNT	BALANCE
12/15/98 9:49:34 AM	ONLINE FINANCIAL NEWS	\$0.50	\$19.50
12/15/98 9:43:08 AM	INITIAL CREDIT CARD DEPOSIT	\$20.00	\$20.00

[\[MAKE DEPOSIT\]](#)
[\[MAKE WITHDRAWAL\]](#)
[\[UPDATE ACCOUNT INFO\]](#)  
[\[CLOSE ACCOUNT\]](#)

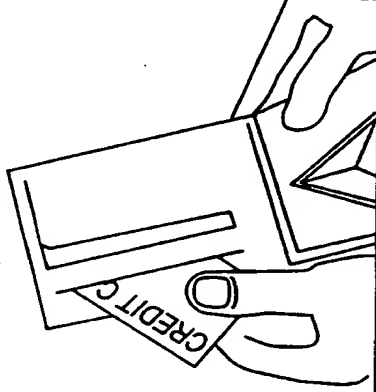


FIG. 21

430



## INTERNATIONAL SEARCH REPORT

International application No.  
PCT/US99/05368

## A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) : G06F 153/00

US CL : 705/26

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 705/26, 27

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,870,473 A (BOESCH ET AL.) 09 FEBRUARY 1999, COL 61, LINE 55 TO COL 64, LINE 43.	1-16
A	US 5,864,667 A (BARKAN) 26 JANUARY 1999, COLUMN 3, LINE 2 TO COLUMN 4, LINE 52.	1-16
A,P	US 5,848,400 A (CHANG) 08 DECEMBER 1998, COLUMN 3, LINE 1 TO COLUMN 7, LINE 17.	1-16
A,P	US 5,815,657 A (WILLIAMS ET AL.) 29 SEPTEMBER 1998, COLUMN 12, LINE 11 TO COLUMN 18, LINE 30.	1-16

☐ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:	*T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
*A* document defining the general state of the art which is not considered to be of particular relevance	*X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
*E* earlier document published on or after the international filing date	*Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
*L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	*G* document member of the same patent family
*O* document referring to an oral disclosure, use, exhibition or other means	
*P* document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search

28 JUNE 1999

Date of mailing of the international search report

02 AUG 1999

Name and mailing address of the ISA/US  
Commissioner of Patents and Trademarks  
Box PCT  
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer

FRANTZY POINVIL

Telephone No. (703) 305-9779

**THIS PAGE BLANK (USPTO)**

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

**THIS PAGE BLANK (USPTO)**